THE RUGBY BOROUGH COUNCIL

An ordinary meeting of the Rugby Borough Council will be held via Microsoft Teams at 6.00pm on Tuesday 15 December 2020.

Members of the public may view the livestream of the meeting via the link on the Council's website.

Mannie Ketley
Executive Director

A G E N D A

PART 1 – PUBLIC BUSINESS

1. Apologies for absence.

2. Minutes.

   To approve the minutes of the meeting of Council held on 26 November 2020.

3. Declaration of Interests.

   To receive declarations of -

   (a) non-pecuniary interests as defined by the Council's Code of Conduct for Councillors;

   (b) pecuniary interests as defined by the Council's Code of Conduct for Councillors; and

   (c) notice under Section 106 Local Government Finance Act 1992 - non-payment of Community Charge or Council Tax.

4. To receive the Mayor's Announcements.

5. Questions pursuant to Standing Order 10.

6. To receive the reports of Cabinet and Committees which have met since the last meeting of the Council and to pass such resolutions and to make such orders thereon as may be necessary:

(a) Cabinet – 7 December 2020

(1) Council Tax Reduction Scheme 2021/22 – Communities and Homes Portfolio Holder.

(b) Audit and Ethics Committee – 10 November 2020

(1) Statement of Accounts 2019/20.

7. To receive and consider the Reports of Officers.

(a) Information Governance and Agile Working Policies – report of the Head of Communities and Homes.

(b) Licensing Act 2003 – Statement of Licensing Policy 2021-2026 – report of the Deputy Executive Director.

8. Notices of Motion pursuant to Standing Order 11.

(a) "This Council congratulates St. Andrew's Church on its forthcoming 800th anniversary as a parish and civic church. The earliest record of a priest serving in Rugby is from 1221 and the church's west tower was built during the reign of Henry III (1216–1272) to serve a defensive as well as religious role and is Rugby's oldest building.

The church was altered and enlarged in the late 19th century to include a new east tower with a high spire. St. Andrew's Church is the only parish church in the world with two sets of bells, numbering 13 in total, one set being in each of the two towers. The church houses other artefacts of medieval Rugby including the 13th century parish chest and a medieval font.

St. Andrew's Church is one of only five churches in the country to have been awarded an Eco-gold award. The church has expressed its thanks to Rugby Borough Council and Warwickshire County Council for their help in working to achieve that award.

St. Andrew's Church is recognised as one of the major churches of England and its contribution to the civic, the cultural and the economic life of the parish and borough demonstrates that. The church is now looking forward to the next chapter in its development. It has aspirations to be given the honorific title of 'Minster'.

We urge this Council to:

(a) support St Andrew's Church in its bid to become a Minster; and
(b) write to the Bishop of Coventry to support the application.

Proposer: Councillor Sandison
Seconder: Councillor McQueen

9. Correspondence.

10. Common Seal.

To order the affixing of the Common Seal to the various orders, deeds and documents to be made or entered into for carrying into effect the several decisions, matters and things approved by the Council and more particularly set out in the Committees' Reports adopted at this meeting.

11. Motion to Exclude the Public under Section 100(A)(4) of the Local Government Act 1972.

To consider the following resolution:

"under Section 100(A)(4) of the Local Government Act 1972 the public be excluded from the meeting for the following item on the grounds that it involves the likely disclosure of information defined in paragraph 3 of Schedule 12A of the Act."

PART 2 – EXEMPT INFORMATION

1. To receive the private reports of Cabinet and Committees which have met since the last meeting of the Council and to pass such resolutions and to make such orders thereon as may be necessary:

(a) Cabinet – 7 December 2020

(1) Newbold Quarry Exemption Report – Environment and Public Realm Portfolio Holder.

DATED THIS 7th day of December 2020

To: The Mayor and Members of Rugby Borough Council

QUESTIONS AT COUNCIL

A Councillor may ask a Question at the meeting by giving notice in writing of the Question to the Executive Director no later than midday on Wednesday 9 December 2020. The rules relating to Questions are set out in Standing Order 10 of Part 3a of the Constitution.

Agenda No 6(a)

REPORT OF CABINET

7 December 2020

PRESENT:

Councillors Lowe (Chairman), Mrs Crane, Poole, Ms Robbins, Roberts and Mrs Simpson-Vince.

Councillors Bearne, Cranham, Douglas, Gillias, Miss Lawrence, Mrs O'Rourke, Picker, Roodhouse, Sandison and Srivastava were also in attendance.

Note: An electronic version of the Cabinet reports referred to below can be found here.

1. INTRODUCTION

Cabinet on 7 December 2020 considered the following item and made recommendations to Council as detailed below.

2. COUNCIL TAX REDUCTION SCHEME 2021/22

Cabinet considered a report concerning the Council's Council Tax Reduction Scheme for 2021/22.

2.1 Recommendation of Cabinet

Cabinet decided to recommend to Council that the Council Tax Reduction Scheme for 2020/2021 be adopted as the Council's Local Council Tax Reduction Scheme for 2021/2022.

Recommendation

The recommendation of Cabinet be approved.

COUNCILLOR S LOWE
CHAIRMAN

Agenda No 6(b)

AGENDA MANAGEMENT SHEET

Report Title:	Statement of Accounts 2019/20
Name of Committee:	Council
Date of Meeting:	15 December 2020
Report Director:	Chief Financial Officer
Portfolio:	Corporate Resources
Ward Relevance:	All
Prior Consultation:	N/A
Contact Officer:	Jon Illingworth, Interim Chief Financial Officer, Tel 01788 533410, jon.illingworth@rugby.gov.uk
Public or Private:	Public
Report Subject to Call-In:	No
Report En-Bloc:	No
Forward Plan:	No
Corporate Priorities: **(CR) Corporate Resources** **(CH) Communities and Homes** **(EPR) Environment and Public Realm** **(GI) Growth and Investment**	This report relates to the following priority(ies): ☒ To provide excellent, value for money services and sustainable growth ☒ Achieve financial self-sufficiency by 2020 ☐ Enable our residents to live healthy, independent lives ☒ Optimise income and identify new revenue opportunities (CR) ☒ Prioritise use of resources to meet changing customer needs and demands (CR) ☒ Ensure that the council works efficiently and effectively (CR) ☐ Ensure residents have a home that works for them and is affordable (CH) ☒ Deliver digitally-enabled services that residents can access (CH) ☐ Understand our communities and enable people to take an active part in them (CH) ☐ Enhance our local, open spaces to make them places where people want to be (EPR) ☐ Continue to improve the efficiency of our waste and recycling services (EPR) ☐ Protect the public (EPR)

	☐ Promote sustainable growth and economic prosperity (GI) ☐ Promote and grow Rugby's visitor economy with our partners (GI) ☐ Encourage healthy and active lifestyles to improve wellbeing within the borough (GI) ☐ This report does not specifically relate to any Council priorities but
Statutory/Policy Background:	The Local Audit and Accountability Act 2014 and Accounts and Audit Regulations 2015, The Code of Audit Practice, Accounts and Audit (Coronavirus) (Amendment) Regulations 2020
Summary:	To present to Statement of Accounts to Council
Financial Implications:	As detailed in the financial statements
Risk Management Implications:	As detailed in the financial statements
Environmental Implications:	There are no environmental implications for this report.
Legal Implications:	The Local Audit and Accountability Act 2014 and Accounts and Audit Regulations 2015, The Code of Audit Practice, Accounts and Audit (Coronavirus) (Amendment) Regulations 2020 require the approval of the statutory Statement of Accounts by 30 November.
Equality and Diversity:	There are no equality and diversity implications for this report.
Options:	None
Recommendation:	The report be noted.
Reasons for Recommendation:	None

Agenda No 6(b)

Council - 15 December 2020

Statement of Accounts 2019/20

Public Report of the Audit and Ethics Committee

Recommendation

The report be noted.

1. Purpose of the report

1.1. The responsibility for approving the annual Statement of Accounts is delegated to the Audit and Ethics Committee. For the year ending 31 March 2019 this took place on 10 November and minutes included a recommendation that the document be submitted to Council for noting.

2. Background

2.1. The Accounts and Audit (Coronavirus) (Amendment) Regulations 2020, require authorities to prepare Statement of Accounts (the accounts) in accordance with proper practices. These require that the Accounts are prepared by 31 August and approved and published by 30 November after the end of the financial year. In comparison the deadlines in 2018/19 were 31 May and 30 September respectively.

2.2. The draft 2019/20 accounts were signed by the Interim Chief Financial Officer on 29 June 2020 and published on the Council's website on 1 July in line with the revised deadline.

2.3. The accounts have been subject to external audit by Grant Thornton LLP and final audited accounts were presented to the Audit and Ethics Committee for its consideration and approval on 10 November.

2.4. An unqualified opinion on the financial statements and the audit certificate were issued on 30 November 2020

2.5. The link below is to the report to Audit & Ethics Committee which includes the Statement of Accounts and the audit findings report.
Audit and Ethics Committee Agenda 10.11.2020

2.6. The link below is a copy of the minutes of the Audit and Ethics Committee
Minutes of the committee 10.11.2020

2.7 The link below is to a copy of the published Financial Statements
Published 2019.20 Statement of Accounts

Name of Meeting: Council

Date of Meeting: 15 December 2020

Subject Matter: Statement of Accounts 2019/20

Originating Department: Corporate Resources

DO ANY BACKGROUND PAPERS APPLY ☐ **YES** ☐ **NO**

LIST OF BACKGROUND PAPERS

Doc No	Title of Document and Hyperlink

The background papers relating to reports on planning applications and which are open to public inspection under Section 100D of the Local Government Act 1972, consist of the planning applications, referred to in the reports, and all written responses to consultations made by the Local Planning Authority, in connection with those applications.

☐ Exempt information is contained in the following documents:

Doc No	Relevant Paragraph of Schedule 12A

Agenda No 7(a)

AGENDA MANAGEMENT SHEET

Report Title:	Information Governance and Agile Working Policies
Name of Committee:	Council
Date of Meeting:	15 December 2020
Report Director:	Head of Communities and Homes
Portfolio:	Communities and Homes
Ward Relevance:	None
Prior Consultation:	Senior Management Team, Legal Services, Head of Communities and Homes, Interim Chief Finance Officer, Employee Network, Trade Unions, Coronavirus Tactical Group, Corporate Management Forum
Contact Officer:	Chris Green, Corporate Assurance and Improvement Manager
Public or Private:	Public
Report Subject to Call-In:	Yes
Report En-Bloc:	Yes
Forward Plan:	No
Corporate Priorities: **(CR) Corporate Resources** **(CH) Communities and Homes** **(EPR) Environment and Public Realm** **(GI) Growth and Investment**	This report relates to the following priority(ies): ☐ To provide excellent, value for money services and sustainable growth ☐ Achieve financial self-sufficiency by 2020 ☐ Enable our residents to live healthy, independent lives ☐ Optimise income and identify new revenue opportunities (CR) ☐ Prioritise use of resources to meet changing customer needs and demands (CR) ☒ Ensure that the council works efficiently and effectively (CR) ☐ Ensure residents have a home that works for them and is affordable (CH) ☐ Deliver digitally-enabled services that residents can access (CH) ☐ Understand our communities and enable people to take an active part in them (CH)

	☐ Enhance our local, open spaces to make them places where people want to be (EPR) ☐ Continue to improve the efficiency of our waste and recycling services (EPR) ☐ Protect the public (EPR) ☐ Promote sustainable growth and economic prosperity (GI) ☐ Promote and grow Rugby's visitor economy with our partners (GI) ☐ Encourage healthy and active lifestyles to improve wellbeing within the borough (GI) ☐ This report does not specifically relate to any Council priorities but
Statutory/Policy Background:	The following areas are relevant: Data Protection Act 2018 Human Rights Act 1998 Freedom of Information Act 2000 Environmental Information Regulations 2004 Copyright, Design and Patents Act 1998 Computer Misuse Act 1990 Regulation of Investigatory Powers Act 2000 Privacy and Electronic Communications Regulations
Summary:	The report sets out a new suite of Information Governance policies, and a new Agile Working policy, for approval.
Financial Implications:	£3,000 of the current year equipment budget has been earmarked to cover costs associated with implementing the Agile Working policy. There is no requirement for a supplementary budget.
Risk Management Implications:	Following approval, the policies might not be effectively and consistently applied. However, to mitigate this risk the Senior Management team has approved arrangements to ensure staff take responsibility for working in accordance with the appropriate policies, and in line with the training being provided. The Information Governance framework includes arrangements for monitoring and oversight.
Environmental Implications:	The Agile Working policy is expected to reduce the carbon footprint of the Council and employees, and will therefore support the response to the Climate Emergency.
Legal Implications:	There are no direct legal implications. However, the policies are designed in part to ensure the

	Council operates in compliance with the legislation set out above under “Statutory/ Policy Background”.
Equality and Diversity:	The Equality and Diversity Officer has reviewed the draft policies. There are no equality and diversity implications arising from this report.
Options:	1. Approve the Information Governance policies, and the Agile Working policy. **Benefits:** The Council implements a consistent good practice framework for managing information governance and agile working. **Risks:** See “Risk Management Implications”. 2. Reject the Information Governance policies, and the Agile Working Policy. **Benefits:** None. **Risks:** Inconsistent approach to managing staff who are already working “agile”. Inconsistent approach to considering and agreeing future agile working requests from staff. Health and safety, data protection, information governance and wellbeing risks not effectively managed. Benefits of agile working not being realised with employee performance not being effectively managed.
Recommendations:	1. The Agile Working policy, as set out at Appendix 1, be approved; 2. the Information Governance Framework, as set out at Appendix 2, be approved; 3. the updated Clean Desk policy, as set out at Appendix 3, be approved; 4. the updated Data Protection policy, as set out at Appendix 4, be approved; 5. the Sharing Information Safely policy, as set out at Appendix 5, be approved; and 6. the Information Security policy, as set out at Appendix 6, be approved.
Reasons for Recommendations:	To enable implementation of a consistent good practice framework for managing information governance and agile working.

Agenda No 7(a)

Council - 15 December 2020

Information Governance and Agile Working Policies

Public Report of the Head of Communities and Homes

Recommendation

1. The Agile Working policy, as set out at Appendix 1, be approved;
2. the Information Governance Framework, as set out at Appendix 2, be approved;
3. the updated Clean Desk policy, as set out at Appendix 3, be approved;
4. the updated Data Protection policy, as set out at Appendix 4, be approved;
5. the Sharing Information Safely policy, as set out at Appendix 5, be approved; and
6. the Information Security policy, as set out at Appendix 6, be approved.

1 Background

1.1 An internal audit review, completed in 2019, highlighted a number of significant gaps in the Council's information governance framework. The Information Governance Group developed an action plan and was working through this to develop a new framework. The Information Governance Group comprises the following officers:

Raj Chand – Head of Communities and Homes, Senior Information Risk Owner and Chief Information Officer
Chris Green – Corporate Assurance and Improvement Manager (Chief Auditor)
Jeremy Carter – Corporate ICT Manager
Matthew Deaves – Communications and Consultation Manager

1.2 It was also recognised that the Council's workforce was gradually becoming more "agile", for example with more employees undertaking some of their duties at home. By the time the current pandemic started there were circa 50 employees undertaking at least some of their duties offsite, predominately from home. Such arrangements were being agreed and managed locally.

1.3 It was accepted that the Council needed to develop and implement an Agile Working policy which recognised the evolving ways of working, and work had commenced on this prior to the current pandemic. However, the arrival of the pandemic brought an immediate step change, with circa 250 employees suddenly asked in March 2020 to work from home.

1.4 This step change in working meant that plans for developing and implementing an information governance and agile working framework needed to be accelerated. Accordingly the Head of Communities and Homes and Senior

Information Risk Owner (SIRO/CIO) established and stood up a “Policy Cell” group to drive forward this work.

2 Policy Development Process and Consultation

2.1 The policy cell was led by the Corporate Assurance and Improvement Manager with support from the Head of Communities and Homes. Members of the policy cell were selected to ensure appropriate expertise and involvement:

- The Communications, Consultation and Information Manager (Data Protection Officer).
- The Corporate ICT Manager
- The Equality & Diversity Officer
- Representatives from HR
- The IT Trainer
- The Safety & Resilience Manager
- The Construction Project Manager

2.2 Progress was monitored by the Head of Communities and Homes and reported regularly to the Coronavirus Tactical Group.

2.3 Extensive consultation has been carried out on the new policies with the following groups included in the process in addition to members of the policy cell:

- The employee network.
- The Trade Unions.
- Legal Services.
- Tactical Group.
- All members of the wider Corporate Management Forum.
- Senior Management Team.

2.4 The information governance policies have also been subject to independent external review by the Council’s appointed IT auditors. This provides assurance that the policies are in line with good practice. Whilst there were some minor suggestions which have all been considered and incorporated where necessary, the auditor has confirmed that the policies are “very strong”.

3 Agile Working Policy

3.1 The Agile Working Policy is set out at Appendix 1. The policy is designed to provide a framework for consistent and fair practice and to address issues that should be considered when managing employees and implementing agile working agreements. The policy is also written in a way which enables it to be applied both in situations where staff wish to apply for agile working as an option, or where the Council needs to implement agile working, for example during the current pandemic or for other strategic or operational reasons.

3.2 There are three areas where a small amount of additional expenditure is expected to be incurred to implement the new Agile Working policy. These relate to the purchase of desks and storage cabinets, and provision of headsets. In the vast majority of cases staff who have been working agile since March 2020 have adapted to the new circumstances. All staff IT equipment

needs, and most other equipment needs, have already been met. Based upon a review of completed Display Screen Equipment (DSE) assessments it is estimated that additional equipment expenditure of up to £3,000 may be required to implement the Agile Working policy. These costs can be met from current year equipment budgets.

4 Executive Summary – Information Governance Policies

4.1 The information governance policies have been developed by the Policy Cell, consulted upon as outlined above, reviewed and approved by the Head of Communities and Homes as the Council's Senior Information Risk Owner (SIRO/CIO). They have also been approved by the Senior Management Team. There are in total 5 information governance policy documents and each is summarised in the following paragraphs, including where applicable the key changes compared with existing documents.

4.2 Information Governance Framework - Appendix 2

An internal audit review in 2019 highlighted a need for the Council to document its information governance framework, and before the current pandemic struck the information governance group had been working on the framework's development. This work was accelerated and concluded by the Policy Cell. The framework is a new document and is the overarching umbrella document underpinned by the various supporting policies and procedures.

The framework document sets out the information governance roles, responsibilities and accountabilities of key officers and member/ officer groups including:

- Executive Director and the Senior Management Team
- The SIRO/CIO
- Information Governance Group
- Corporate ICT Manager
- Information Asset Owners (service managers)
- Strategic Risk Management Group
- Audit & Ethics Committee
- Employees/ other parties

Specifically, the Executive Director and Senior Management Team are responsible for:

- ensuring a comprehensive information governance framework, policies, standards, procedures, and systems are in place and operating effectively throughout the Council.
- Preparing information governance assessments and action plans as part of the Council's overall Annual Governance Statement and updating the information risk assessment.
- Monitoring the work of the Information Governance Group, including compliance and improvement activities across the Council.
- Monitoring information handling and breaches, implementing assurance arrangements and taking corrective actions.
- Ensuring that training and action plans for information governance are progressed throughout the Council and evaluating their effectiveness.

- Communicating the information governance agenda, for example through the Corporate Management Forum and Employee Briefings.

4.3 Clean Desk and Data Protection Policies - Appendices 3 and 4

The Clean Desk policy is already in place, having been developed by the information governance group, approved and circulate to staff. The Data Protection policy is also already in place having been developed and approved in December 2017 prior to implementation of the General Data Protection Regulation. There are no substantive changes to either policy. However, they have been reviewed and reformatted to ensure consistency with the other documents in the framework. Following approval these policies will be recirculated and their importance emphasised particularly for staff who are working “agile”.

4.4 Sharing Information Safely Policy Appendix 5

The internal audit completed in 2019 highlighted that there was no policy in place to outline the Council’s approach to data minimisation and pseudonymisation. Accordingly, a policy has been developed for implementation within the new information governance framework. The policy enables the Council to undertake secondary use of personal data in a safe, secure and legal way. Through a number of channels the Council collects customer information such as name, address, and date of birth. However, if those identifiable details are removed, information can be used for secondary purposes without fear of breaching the General Data Protection Regulation. This process is called anonymisation.

The purpose of this policy is to ensure a standardised approach to enable consistency throughout the Council, with regard to how and when to anonymise information correctly. Anonymisation is the process of removing, replacing and / or altering any identifiable information (identifiers) that can point to the person(s) it relates to. Pseudonymisation is the technical process of replacing the identifying information to protect the individual’s identity whilst allowing the recipients to link different pieces of information together. A nickname is an example of pseudonymisation.

Under the policy anyone considering anonymisation should test to find out whether information in the anonymised dataset could be combined with searches of easily available information to reveal the identity of individuals. Examples might include the electoral register or social media. The policy contains detailed guidance for staff on how to effectively anonymise or pseudonymise data.

4.5 Information Security Policy Appendix 6

The new Information Security policy incorporates and amalgamates in one document the existing Internet, Intranet and Acceptable Email use policy, and IT Security policy. The new policy also covers a number of new areas as follows:

- The requirements of the Data Protection Act 2018 and the GDPR.

- Rules on the use of Council supplied mobile devices, for example reasonable personal use, monitoring arrangements, appropriate usage including downloads, alteration of equipment and management of devices.
- Arrangements to manage risks arising from the use of Cloud services and the risk of cyber crime. This includes the consequences for employees should they undertake activity which causes or could cause computer systems, information or networks to be compromised.
- Management and classification of information including hardcopy materials.
- Arrangements for managing physical access.

5 Next Steps – Training

5.1 Once the policies have been approved and finalised, staff will be advised of this via InTouch and the policies will be placed in a dedicated area on the Intranet.

5.2 The policies will then be circulated individually via Metacompliance. The IT Trainer is developing a short training video with a test for each policy, to help staff absorb and understand the content. This will be undertaken over a period of around 3 months to avoid inundating staff with multiple requests to read and understand new material at the same time.

5.3 Finally, the Way We Manage training programme will be amended to incorporate, within one of the existing sessions, training for managers on the content and application of the new Information Governance policies, and Agile Working policy and guidance.

5.4 Once the policies have been approved, the Policy Cell will be stood down having served its purpose. However, the Corporate Assurance and Improvement Manager will monitor the policies' implementation and ensure the training is rolled out as planned.

6 Conclusion

6.1 Council is asked to approve the new suite of policies to enable implementation of a consistent good practice framework for managing information governance and agile working.

Name of Meeting: Council

Date of Meeting: 15 December 2020

Subject Matter: Information Governance and Agile Working policies

Originating Department: Communities and Homes

DO ANY BACKGROUND PAPERS APPLY ☒ **YES** ☐ **NO**

LIST OF BACKGROUND PAPERS

Doc No	Title of Document and Hyperlink
1	Agile Working policy
2	Information Governance framework
3	Clean Desk policy
4	Data Protection policy
5	Sharing Information Safely policy
6	Information Security policy

The background papers relating to reports on planning applications and which are open to public inspection under Section 100D of the Local Government Act 1972, consist of the planning applications, referred to in the reports, and all written responses to consultations made by the Local Planning Authority, in connection with those applications.

☐ Exempt information is contained in the following documents:

Doc No	Relevant Paragraph of Schedule 12A

AGILE WORKING POLICY

Introduction

Agile working is a method of working to enable our employees to work where, when and how they choose, with maximum flexibility and minimum constraints. It can help to optimise employee performance and deliver the best value and customer service. It uses communications and information technology to assist employees to work in ways which best suit their needs without the traditional limitations of where and when tasks must be performed.

Agile working is based on the concept that work is an activity that employees undertake, rather than a location they physically go to. With the technology available, there are numerous tools to facilitate working in new and diverse ways, to meet our customer needs, reduce costs, increase productivity and improve sustainability.

Agile working is a transformational tool which allows employees to work smarter, eliminating all barriers and to work more efficiently. In addition, it will improve employee's ability to maintain a healthy work/life balance.

Due to the Covid-19 pandemic in 2020, the implementation of an Agile Working policy was brought forward in order to adapt, provide a continuous and seamless service to our customers and provide additional COVID safe working practices for our employees.

Purpose

The policy provides a framework for consistent and fair practice to address issues that should be considered when managing employees and implementing agile working agreements.

This policy enables our employees to gain a better understanding of agile working, the basic principles to be considered and how it is applied to varying types of roles.

Scope

- This policy applies to all permanent & fixed term contracted employees of Rugby Borough Council.
- The nature and extent of agile working will depend upon the job undertaken as providing services to customers will be a priority. Not all roles are suitable for agile working.
- The decision to adopt agile working will be mutually agreed by the employee and their Manager, supported by well-defined objectives and performance measures. There may be situations, however, where the Council requires employees to adopt agile working (for example as part of a response to a pandemic or other emergency, or for other operational reasons). In these circumstances the provisions of this policy will apply, except for the agile working application form, which will not need to be completed.
- This policy does not negate or supersede the Council's policy on Flexible Working.
- This policy covers the provision of facilities by the Council to enable employees working for (or on its behalf) to have secure access to any information systems for which they have the authorisation to access.

Definitions

The following definitions apply throughout this document;

Council:	Rugby Borough Council, or Employer.
Employees:	Permanent & Fixed term contractual employees of Rugby Borough Council
Agile Working:	Flexible and more sustainable way of working. Employees are not fixed to one location or desk and have the required tools and systems to work at any location, at any time. The purest form is being able to work any time, any place and in any way.

Agile working can be undertaken in the following work styles:

Home Worker	• Home based for majority of their contracted working week. • Does not have a dedicated workstation at the Town Hall or any other Council location. • Has a fully equipped & DSE compliant workstation at home.
Hot Desk Worker	• Based at the Town Hall or any other Council location for majority of their contracted working week. • Has access to a workstation (allocated for each day or week) at the Town Hall or any other Council location. • **Please note: This working style cannot currently be facilitated by the available Council accommodation.**
Fixed Desk Worker	• Based at the Town Hall or any other Council location for majority of the contracted working week. • Has access to a specific workstation at the Town Hall or any other Council location. • Has specific and/or unique IT application access requirements requiring a fixed workstation • To comply with the Equality Act 2010, a person with a disability who requires reasonable adjustments to be put in place to fulfil their job role, may require fixed DSE compliant equipment.
Remote Worker	• Mobile roamer for most of their contracted working week. • Accesses docking stations/synchronises in various Council &/or non-Council working locations. • Has remote access to Council systems. • Spends most of their contracted working week in a variety of Council &/or non-Council working locations.
Hybrid	• Any combination of the above.

1. Benefits

Agile working, when used effectively, delivers benefits to both the Council and its employees as well as having environmental benefits. It is a flexible and sustainable way of working with employees, provided with the tools to work anywhere, at any time, including the ability to work from home if the employee so chooses (and it has been agreed with the relevant Manager).

Agile working can benefit from matching Council needs with employee's preferred working style. This allows employees to achieve a better work life balance.

Employee applications for agile working will not unreasonably be refused. However, not all employee needs can be met as there is an overarching requirement to provide Council services at the necessary times and places. Furthermore, employees with an agile working arrangement in place may still be required to attend their place of work, for example for face to face meetings or to fulfil any physical obligations of their role.

1.1. Employee benefits include:

- Potential for reduced travel costs and travel time
- Potential for reducing stress (due to less travel)
- Potential for increasing free time (due to less travel)
- Increased flexibility in working life
- The ability to work at home on a specific piece of work, avoiding the interruptions that can be part of the office environment
- Increased sense of value as a result of autonomy and trust at work
- Increase in wellbeing and health – reduced stress, better sense of control, ability to integrate exercise into the day more easily, etc.
- Increased personal performance due to more efficient ways of working, leading to a greater sense of achievement.

1.2. Council benefits include:

- Reduction in the need for office accommodation
- Provision of a more efficient and effective service, due to fewer interruptions and the flexibility to adapt to an employees' preference of working style.
- New employee attraction.
- Existing employee retention.
- Use home working for a temporary period as a means of helping an employee return to work following a long-term illness, minimising injury risk to those who are vulnerable.
- Enable learning and development activity to be undertaken remotely, including e-learning.
- Enable the council to respond to an individual's need for flexibility in working arrangements, for example, to support employees with responsibilities as carers.
- Provide alternative solutions to short or longer-term office accommodation issues including a reduction in running costs.
- Reduction in organisation and personal carbon footprint.

- Increased motivation and engagement of employees.
- Improved business continuity including less disruption and employee absences due to weather, travel problems, etc.

2. Responsibilities

2.1. Managers will ensure the following:

- The procedure is complied with and applied effectively, fairly and consistently within their area of responsibility.
- Regular contact/communication is maintained with team members through both individual and team meetings, providing support for employees and implementing ways of measuring performance and in compliance with lone working safeguarding.
- Make sure the Employees well-being needs are being met. For example; encouraging them to maintain social contact with colleagues, sign posting them to the Mental Health SharePoint pages and recommending referrals to Occupational Health, or confidential counselling services if appropriate.
- Have identified and agreed a work base location from which employees can work with support and have use of facilities & provision of office consumables, appropriate to the job role.
- Employees have access to suitable training to enable them to work effectively and identify any additional training needs as a result of agile working.
- Employees have followed health and safety guidelines, such as completing a risk assessment for each set up of display screen equipment and workstation, as well as completion of the DSE e-learning module and a lone worker risk assessment. All issues highlighted must be recorded and the remedy co-ordinated by the Manager. Records will be retained and reviewed in line with data retention guidelines.
- Agree adequate & appropriate team cover to ensure there is sufficient service coverage during core office hours and that customer service standards are not negatively impacted as a result.

2.2. Employees should be aware and understand the following:

- Performance and productivity expectations and targets will be agreed.
- The method for measuring workload, performance and productivity. For example, the regular 1:1 meeting between employee and Manager.
- The method and regularity of communication between self, Manager and colleagues will be agreed.
- The need to support and assist colleagues, as when working in the workplace.
- Requirement to record hours worked and breaks. For example, on a flexi time sheet.
- Make sure their well-being needs are being looked after as when based in the workplace. For example; seeking further advice and guidance via the Well Being pages on Sharepoint,

creating a well-being action plan, speaking to one of the Mental Health First Aiders, accessing the confidential counselling service as well as maintaining social contact with colleagues and Line Manager.

In addition, employees must:

- Take responsibility for Council equipment assigned to them when working in differing locations, particularly including the security & protection of Council &/or personal data. Any loss, damage or theft must be immediately reported to both IT and your Manager.
- Follow health and safety guidelines, such as completing a risk assessment for each set up of display screen equipment and workstation, as well as completion of the DSE e-learning module and a lone worker risk assessment. All issues highlighted will be recorded and the remedy co-ordinated by the Manager. Records will be retained and reviewed in line with data retention guidelines.
- Where possible, move regularly from a single work setting & take regular screen breaks to gain benefit from a change of posture.
- Take breaks in accordance with the Working Time Regulations. Any employee who works more than 6 hours in a day must have a minimum 30-minute break (in accordance with the Council's flexi-time policy). This break must be taken during the working day, before 6 hours of working have passed, and, not at the end of the working day.
- Must attend team meetings and maintain communication between themselves and other team members as required
- Must ensure that they log out of all Council ICT systems at the end of each working day.
- Manage their work-related travel and limit it in order to maximise the environmental benefits of agile working.
- Ensure when working from home, that they have a secure and adequate internet connection. Where an employee cannot connect to the Council's ICT network (e.g. central Citrix facilities) it is their responsibility to contact the IT team, travel to their contracted office location or contact their Manager for assistance.
- Where employees have their own personally adapted equipment (e.g. Larger screens for visual impairments) they will be able to move it with them when working at other locations.
- Where employees have specially adapted equipment they are advised to work from their base office if working elsewhere could compromise their health and safety.

3. Operational Requirements

3.1. Support

Both Managers and employees must ensure that working arrangements are effective and deliver the best possible customer service. Managers must continue to support employees and both parties are responsible for maintaining good working relationships.

3.2. Communication

Managers must put arrangements in place to ensure that all information is openly and frequently shared and that employees remain briefed of corporate and team developments. Managers must also consider mechanisms for communication and networking between team members and other

relevant parts of the Council. Managers may need to put in more regular contact with employees that are lone working at home which will be determined by a Lone Worker risk assessment.

3.3. Absence Reporting

The Council's Absence Management Policy applies to all employees regardless of their working arrangements. All employees must follow the sickness reporting process contained within the policy.

In the event of an incident, it is important to be able to ascertain if an employee was working, or not working. This is for both health & safety and legal reasons when an employees does not have in place a fixed agile working pattern. All accidents, incidents, near misses whilst working must be reported via the RBC Incident reporting procedure.

3.4. Performance Management

There should be well defined and agreed performance objectives and goals, set by Managers. These need to be communicated and regularly reviewed by Managers and employees through regular contact, for example within the 1:1 meeting.

3.5. Equipment

The Council will supply equipment needed to enable each employee to work effectively in their respective work styles. IT and communications equipment must not be used by anyone other than the employee who is authorised to do so.

Home telephone and broadband connections are the responsibility of the Employee. IT Service Desk will not contact home telephony/broadband suppliers to investigate technical and availability issues.

The Council will not pay for any unapproved IT &/or communication equipment or office chairs which an employee privately purchases, regardless of whether or not it is to be used within the scope of their job role. All IT equipment required for the role, and including office chairs, will be provided by the Council. For clarity of communication and data protection purposes, the use of headsets is encouraged. These should only be procured through the IT department.

Where an employee is working at home or remotely, and where a DSE assessment has indicated a change or a new DSE requirement, an employee may reclaim via the Expenses process, up to £150.00 towards to the cost of an approved new desk. Reimbursement can only be made once.

The Council will not pay for smoke alarms, fire extinguishers, first aid kits, or for any repairs to correct electrical defaults in the employee's home.

Employees should note that if they leave the Council within a 12-month period following the date of reimbursement, they will be expected to repay the cost of any DSE equipment not returned to the Council by deducting the cost reclaimed from the employee's final salary.

All Council policies apply to all employees regardless of their work style, including but not limited to; all HR policies, Data Protection and the IT Security Policy.

3.6. Business Mileage and Subsistence

The Council's Car Allowance and Employee Allowances and Expenses Policy will apply to all employees for reimbursement of mileage and business consumables, where appropriate.

All employees will continue to have a designated base for travel claim purposes. This will be an existing Council location, unless the employee is a home worker in which case the designated base will be the employee's home address.

3.7. Security of Data

All data used must be secure in order to ensure compliance with the General Data Protection Regulation 2016.

The Council's default position is that staff who are working "agile" should do so by electronic means wherever possible. Use and storage of paper records away from the office is discouraged and home printing devices are not supported by the ICT department. If you currently need to use and/or store hardcopy documents to fulfil your role, then please contact the IT department in the first instance to discuss if this could be digitalised.

It is recognised, however, that there may be exceptions where it is necessary to store small amounts of hard copy confidential records at home for short periods of time. In such circumstances, and where the employee does not already have secure storage available, the Council may at its discretion reimburse employees for receipted expenditure of up to £50 on a small lockable storage cabinet. There must be a demonstrable business need and a Data Privacy Impact Assessment must be carried out. This should not be viewed as an allowance.

Employees should in no circumstances dispose of hard copy confidential documents in their domestic waste; such records should be safely and securely disposed of on Council premises.

In addition to following the requirements of the Clean Desk policy, employees who are appearing on camera for meetings, should ensure that the background is appropriate for a work environment.

Employees must continue to comply with the requirements of the Council's Data Protection policy, It Security policy, Sharing Information Safely policy & the IT guide to working from home, which are located on SharePoint.

3.8. Training and Development

Managers must ensure that all employees continue to receive appropriate training in all areas to ensure the delivery of an efficient and effective service. It is important that all employees have access to regular training and development opportunities, including team development. Where required employees must attend training and development activities at the designated location.

3.9. Changing an existing Work agreement

The working agreement may be amended either permanently or temporarily as a result of:

- An employee moving into a different position within the Council.
- An employee making a request to change their working agreement. In this event, the change will need to be agreed between the Manager and employee and will not have a detrimental effect on performance or service delivery. It will also be dependent on availability of the appropriate IT equipment.
- Where the current working arrangements are not meeting business needs.
- An employee returning from a long-term sickness absence.
- An employee being performance managed under the Capability policy and procedure.
- An employee being subject to an internal disciplinary or grievance investigation.

3.10. Housekeeping

Desk & office facilities may be used by other employees, so it is essential that a "clear desk approach" needs to be adhered to in accordance with the Clear Desk policy. All desks, office, telephones & IT equipment must be left in an acceptable manner for other users. The Clear desk policy sets out how employees should store their equipment & documentation at the end of each working day.

3.11. Hours of Work/Availability

- Employees and Managers must agree specific working patterns. Most teams will operate within the Flexitime Scheme. In any event, any request to vary an agreed working pattern must be agreed in advance by the Manager.
- If an employee is working from their home address, their availability times must be agreed. Any requirements of the employee to make contact with the Manager/office must also be communicated and the employee should ensure that they are contactable during the agreed hours by email telephone and/or by other communication methods, for example MS Teams.
- Employees should observe the guidance detailed in the Flexitime policy. For example; taking appropriate rest breaks when working for longer than six consecutive hours.
- The Flexitime policy and procedure still apply for all types of working arrangement. Arranged cover for usual office opening hours 0900 to 1700 hours, Monday to Friday, should be provided by the team. There will normally be restrictions on earliest start and latest finish time due to timings when different Council locations are open. However, these restrictions do not need to apply when working from remotely but availability and cover for the service &/or department must take priority. Cover requirements are normally co-ordinated by the Manager who will continue to monitor flexitime records for their employees regardless of working style.
- It should be noted that the IT Helpdesk **will not** be available 24/7 if any issues arise.
- All Employees have the right to privacy out of hours. There must be clarity about the times during which an Employee is available for contact and when / how often they should make contact with their Manager/office.
- It is likely that many meetings will take place at the Town Hall or any other Council location. Managers can also request employees to attend meetings at different venues, attend the office or be part of an audio/video conference remotely if required.
- Home & hybrid workers must retain the flexibility to attend the Town Hall or any other Council location to provide cover for annual leave or sickness absence and should not make personal commitments that could not be changed. For example, an employee should not commit themselves to caring for a dependant if this would not enable them to attend their office location if requested or required to do so.

3.12. Time Recording

Working hours must be recorded in line with the Council's Flexitime policy and procedure; including deducting breaks from work for private appointments to make up contractual weekly working hours.

Travel time to and from an employee's contracted work location should not be included as working time. Travel time to other Council or customer locations is counted within weekly working time. However, when undertaking these journeys from home, the equivalent time of the journey to and from to the employee's contracted work location should be deducted from the total travelling time.

4. Health and safety requirements

4.1. Health and Safety at Work Act 1974 (HSWA)

It is the duty of the Council to ensure, so far as is reasonably practicable, the health, safety and welfare at work of all employees. Suitable and sufficient risk assessments must be carried out by the employer. The purpose is for management to consult with employees to identify hazards, assess the probability that harm may arise from them and evaluate the effectiveness of control measures.

All employees of the Council have a duty while at work to take reasonable care for the health and safety of both themselves and of other persons who may be affected by their acts or omissions at work; and to co-operate with the Council or other persons so far as is necessary to enable them to perform their duties or requirements under the HSWA.

4.2. Health and Safety Risk Assessment

- To comply with all relevant health and safety legislation, the Council must undertake appropriate risk assessments, including, Lone Worker assessments and a DSE assessment for every working location, for each employee who has an agile working agreement.
- These risk assessments will look at the employee's work activities, equipment and environment, and if necessary, action will be taken; this could include permanently or temporarily suspending or amending an agile working arrangement.
- All workstations within the Town Hall or any other Council location are compliant with all relevant DSE requirements but will have specific individual adjustments if appropriate.
- A DSE and a lone worker risk assessment should be carried out by any employee who is working from home. Employees who work from two locations e.g. home and the Town Hall or any other Council location on a regular basis will be required to be complete a DSE assessment for each working location.
- The DSE assessment will need to be carried out again if any substantial changes are made to the working environment or arrangements. Employees must fully participate in completing the necessary risk assessment paperwork and review this with their Manager.
- Home and hybrid workers who do not have a fixed desk arrangement will be provided with information, training and guidance to enable them to set up their workstation wherever they may be working.
- Due consideration to lone working arrangements should be explored fully between the Manager and employee to ensure safe working arrangements are in place.
- When working from home, even if it is only on an ad-hoc basis, the employee has a responsibility to ensure they have an appropriate workspace with adequate security, storage and reasonable screening from activities and noise in the rest of the home. There must also be adequate ventilation, lighting and heating.
- **For personal safety reasons, face to face meetings with clients or customers MUST not under any circumstances be held at an employees' home address.**

5. Additional information

5.1. Contractual Location

The employee's contractual working location will remain unchanged. Employees who have agile working arrangements which include working from home or from a non-Council location, will continue to have a contractual base at the relevant Council location.

Employees who have a formal & permanent agreement to work from home will have the contractual work base stated as their home address.

5.2. Property and Liability Insurance

- Computers and other items of equipment provided by the Council as part of the agile working arrangement will usually be covered by the Council's insurance. In some circumstances, the Council may decide to ask the employee to claim against their home insurance policy.
- Care and security of equipment should be observed when working both at and away from, the contractual base. Disciplinary action may be taken if there is evidence of negligence by the employee.
- Home & hybrid workers are required to contact their own insurance company to inform them that they will be working at home. This does not usually result in any increase in premium and it is unlikely that working from home will affect cover.
- Risk control measures identified, as a result of risk assessment, must be addressed prior to the agile working arrangement commencing.
- If an employee has any personally adapted equipment that they require in order to undertake their duties, then this will be specifically allocated to them and will be for their use wherever they are working under this arrangement.
- Employees working at or from home are covered by the Council's Employers Liability Policy, but only during the time whilst carrying out their work activities. Any accidents, incidents or near misses must be reported immediately in accordance with the Council's health and safety guidelines.
- Before commencing any working from home, employees should advise mortgagees or landlords that they intend to do so. The Council will not be responsible for any additional costs as a result from non-disclosure to a third party.
- Using a room or part of a room at home to work in would not normally require planning permission.
- Working from home should not affect the calculation of Residential Council Tax.

5.3. Working Agreement Review

- Agile working arrangements should be reviewed as part of the 1:1 process, or earlier if these meetings don't take place regularly.

- If problems arise every effort will be made to resolve them. However, in some cases, it might be necessary to terminate the agile working arrangements. If the arrangements are terminated the employee will revert to their previous working arrangement or new arrangements made by the Manager.
- Managers will only terminate agile working arrangements for sound business or performance reasons and after fully consulting with the employee. The termination should be confirmed in writing.

6. Abuse of the Policy

Agile working will result in reduced or no direct supervision of work completed. A high level of trust and confidence is expected between the Manager and Employee. Where abuse of the policy is suspected, a Manager may carry out monitoring on an employee's workload and activity. Any employee who is found to have abused this policy may be subject to formal disciplinary action. Falsification of working hours could constitute gross misconduct and may lead to dismissal.

7. Modifications

This policy and procedure are non-contractual. It will be periodically reviewed by the Human Resources team, and may be varied from time to time, following consultation with any recognised employee representation bodies.

Policy Published Date:	1st December 2020	**Equality Impact Assessment Completed Date:**	1st July 2020
Policy Owner:	Suzanne Turner	**Policy Reference:**	HRPP-01

Appendix 2

Rugby Borough Council

Information Governance Framework

November 2020

Document History

Version	Date	Notes	Prepared by
0.1	27/09/2020	Draft	Policy Cell
0.2	23/11/2020	Approved by SMT	Policy Cell

Table of contents

1 Introduction

1.1 Information is a vital asset for the provision of services to the public and for the efficient management of Council services and resources. As well as protecting confidentiality and ensuring rights to access public and personal information, it plays a key part in governance, service planning and performance management.

1.2 Information governance is concerned with how information is held, obtained, recorded, used and shared by the organisation to achieve compliance with information governance laws and current best practice.

1.3 Information is used here as a collective term to cover terms such as data, documents, records, web content, images and biometric data.

1.4 It is essential that the Council has a robust information governance management framework, to ensure that information is effectively managed with accountability structures, governance processes, documented policies and procedures, staff training and adequate resources.

2 Purpose

2.1 The purpose of this document is to set out the information governance framework for the Council. It demonstrates the Council's commitment to having in place sound information governance arrangements, gives direction to managers and staff, and will help to ensure that legal requirements and best practice standards are met.

3 Scope

3.1 This framework applies to all types of information and data, both electronic and manual, which is held, processed or transmitted by the Council.

3.2 The framework applies to all elected members, employees and others working on behalf of the Council i.e. partners, contractors, consultants or other agents of the Council who have access to information held by or on behalf of the Council. Non compliance with this framework and associated policies could potentially expose the Council and/ or its customers to unacceptable risk.

4 Roles and Responsibilities

4.1 **Cabinet and Audit and Ethics Committee**

The Cabinet is the lead body responsible for the Council's policy framework and its proper implementation. This includes the information governance framework.

The Audit and Ethics Committee is responsible for oversight of the Council's arrangements for corporate governance and risk management; this includes assessing the effectiveness of the Council's information governance arrangements.

4.2 Executive Director and Senior Management Team

The Executive Director, together with the Senior Management Team (SMT), is responsible for ensuring delivery of effective information governance across the Council. This includes the Information Governance Group (IGG), who lead on Information Management, Information Security and the Data Protection policy. The SMT is responsible for:

- Approving and ensuring a comprehensive information governance framework, policies, standards, procedures, and systems are in place and operating effectively throughout the Council.
- Preparing information governance assessments and action plans as part of the Council's overall Annual Governance Statement, and updating the information risk assessment.
- Monitoring the work of the Information Governance Group, including compliance and improvement activities across the Council.
- Monitoring information handling and breaches, implementing assurance arrangements and taking corrective actions.
- Ensuring that training and action plans for information governance are progressed throughout the Council, and evaluating their effectiveness.
- Communicating the information governance agenda, for example through the Corporate Management Forum and Employee Briefings.

Information Governance will be considered periodically as part of the regular SMT agenda and for the relevant items the Senior Information Risk Owner, Communication Consultation and Information Manager, Corporate ICT Manager, and the Corporate Assurance and Improvement Manager, or their nominated deputies, will also attend the meeting.

SMT will also receive advice and guidance from Internal Audit, Legal Services, and other relevant organisations and officers as it requires.

4.3 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) has overall responsible for managing information risk in the council and is a member of the Senior Management Team. The SIRO is the Head of Communities and Homes, and reports to the Executive Director and Senior Management Team on the IGG's

activities. The responsibilities of the SIRO include:

- overseeing development of the information governance framework and associated suite of policies
- ensuring information governance compliance with legislation and council policies
- providing a focal point for managing information risks and incidents
- preparing and monitoring information risk assessments for the council
- fostering a culture for protecting and using information within the council
- providing the senior management team with periodic updates on information governance risks and issues, and progress towards implementing and embedding the information governance framework.

4.4 **Information Governance Group**

The Information Governance Group consists of:

- The Senior Information Risk Owner (SIRO)
- The Communication, Consultation and Information Manager (Data Protection Officer).
- The Corporate ICT Manager
- The Corporate Assurance and Improvement Manager

The purpose of the Information Governance Group is to provide strategic advice and assurance to the Council on all matters concerning information management governance and assurance. The Group is chaired by the SIRO.

The Communication Consultation and Information Manager will provide expert advice and guidance to all staff on all elements of Information Governance. This role is nominated as the Data Protection Officer and, together with the Information Governance Group, is responsible for:

- Providing advice and guidance on information governance to all staff.
- Developing Information Governance Framework of policies, standards and procedures and the Information Governance Action Plan.
- Working with Information Asset Owners (and their representatives) to establish protocols on how information is to be used and shared.
- Developing Information Governance awareness and training modules for

staff.

- Ensuring compliance with Data Protection, Freedom of information, Records Management, Information Security, and other information related legislation via the regular information audit and register of processing activity update.

- Providing guidance and advice on Privacy Impact Assessments.

- Coordinating and processing corporate information requests, processing requests on behalf of services and supporting information coordinators in other services.

- Integrating Government and Information Commissioner guidance, policies, and codes of practice.

4.5 **Corporate ICT Manager**

The Corporate ICT Manager is the lead for technical security management of the infrastructure and technical security advice, including areas such as: PSN Code of Connection, PCIDSS and device policy.

4.6 **Legal and Democratic Services Manager**

The Legal and Democratic Services Manager is responsible for providing expert legal opinion on all information governance matters to all services

4.7 **Information Asset Owners**

Service Managers are designated Information Asset Owners and are responsible for the management of information risk for their service's information assets. This includes:

- Understanding and addressing the risks to the information assets they "own".

- Knowing what information is held, and understanding the nature and justification of information flows to and from the asset.

- Ensuring that their information assets are properly recorded in the Council's information asset register.

- Knowing who has access to their information assets and why.

- Ensuring access is monitored and kept to the minimum level necessary to satisfy business objectives.

- Ensuring that any risks to the information held are identified and included in the appropriate risk register and effectively managed.

- Ensuring the confidentiality, integrity, and availability of all information that the systems create, receive, maintain or transmit, and protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

- Approving and overseeing the disposal mechanisms for information that is no longer needed.

4.8 **Strategic Risk Management Group**

The Strategic Risk Management Group's role is co-ordinating the management of information risks at the corporate level via the strategic and corporate risk registers.

5 Key Policies

5.1 The key policies in the framework are:

- Information Security Policy
- Data Protection Policy
- Clean Desk Policy
- Agile Working Policy
- Managers Guidance on Agile Working including Risk Assessments
- Sharing Information Safely Policy

These policies are supported by sub-policies, standards and procedures. Outputs will be produced from use of these standards and templates, for example privacy assessments, awareness guides and training material.

6 Governance Framework Accountability

6.1 **Service Area Management Teams**

They are accountable for the effective management of information risk and information governance compliance, as well as supporting and promoting the policies, standards and procedures. The teams comprise of the Heads of Service and Managers for each service area.

6.2 **Council Managers**

Each is an Information Asset Owner who is accountable for information assets within their service. They are able to understand how it is held, used and shared and address risks to the information. They are responsible for updating the Register of Processing Activity as required and at least annually.

6.3 **Lead Officers and Team Leaders**

Lead Officers and Team Leaders are responsible for the implementation and adherence to this policy framework and any associated standards and procedures within their service and teams.

6.4 **Employees and Other Parties**

Disregard for information governance policies by employees may be regarded as misconduct and the council's Dismissal and Disciplinary Procedures will be applied. A serious breach of any information governance policy may be treated as gross misconduct and could lead to dismissal.

Disregard by contractors and agents working for the council will be regarded as a contractual breach. Disregard by volunteers and work experience students working for the council may lead to terminating their work agreement.

7 Training and guidance

7.1 Information Governance training for all staff will be mandatory as part of induction, to include all employees. Managers and Lead Officers will also receive training as part of the Way We Manage Training.

7.2 Further information governance modules as appropriate to employee roles will be available through e- learning on the MetaCompliance system or through recognised providers.

7.3 All staff will be required periodically to complete update/refresher training.

7.4 Awareness sessions may be given to staff as required, at team meetings or other events.

7.5 Regular reminders on information governance topics are made through corporate and local team briefings, staff news and emails.

7.6 Policies, procedures, standards, and advice are available to staff at any time on the RBC Intranet pages.

8 Information Security Incident Reporting

8.1 The Information security incident reporting procedure is available to all staff and is available for download. All information security incidents involving digital or manual records whether actual or suspected, should be promptly reported via the link on the SharePoint home page.

9 Monitoring and Review

9.1 This policy and the supporting standards will be monitored and assessed annually in line with legislation and codes of best practice.

10 Further Information

Communication Consultation and Information Manager,
Town Hall, Evreux Way, Rugby CV21 2RR
Telephone: 01788 533562

11 Appendix 1 Information Governance Framework

	IG Management	Confidentiality	Access to Information	Information Security
Policies	Information Governance Framework	Data Protection Policy Sharing Information Safely Policy Agile Working Policy	Data Protection Policy Sharing Information Safely Policy	Information Security Policy Agile Working Policy
Sub-Policies		Privacy Impact Assessments	Privacy Impact Assessments	
Training and Awareness	There will be a planned approach to training and awareness for each policy. This will be role based, regularly assessed, and should equip each person to fulfil their responsibilities.			

Procedures	N/A		Requests for information	
Compliance	Compliance reporting and monitoring will be undertaken by the Information Governance Group, SMT and the Strategic Risk Management Group.			

12 Appendix 2 - External Legislation and Regulation

Data Protection Act 2018
Data Protection Act 1998
Human Rights Act 1998
Freedom of Information Act 2000
Environmental Information Regulations 2004
Local Government Acts
Copyright, Design and Patents Act 1998
Computer Misuse Act 1990
EU Data Protection Regulation (GDPR) 2016 (applicable from 25 May 2018)
Regulation of Investigatory Powers Act 2000
Privacy and Electronic Communications Regulations

Appendix 3

Rugby Borough Council Clean Desk Policy

November 2020

Document History

Version	Date	Notes	Prepared by
0.1	17/07/2019	Approved for SMT	IGG
0.2	18/09/2020	Review and minor amendments to ensure alignment with the new information governance and agile working policies.	Policy Cell
0.3	23/11/2020	Approved by SMT	Policy Cell

Table of contents

1 Overview

1.1 A clean desk policy can be an important tool to ensure that all sensitive/ confidential materials are removed from an employee workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of data security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information and prepare employees for a future paperless environment, a key directive for a digital workplace.

2 Purpose

2.1 The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees, our intellectual property, our customers and our vendors is secure in locked areas and out of site. A Clean Desk policy is not only ISO 27001/17799 compliant, but it is also part of GDPR requirements.

3 Scope

3.1 This policy applies to all Rugby Borough Council employees and affiliates.

4 Policy

4.1 Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

4.2 Computer workstations must be locked when workspace is unoccupied.

4.3 Computer workstations must be shut down at the end of the workday (unless advised).

4.4 Any "official" or "official sensitive" information must be removed from the desk and locked away when the desk is unoccupied and at the end of the workday.

4.5 File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.

4.6 Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.

4.7 Laptops must be either locked away in a drawer or taken home securely.

4.8 Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

5 Documentation

5.1 All printers should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

5.2 Printouts containing Restricted or Sensitive information should be immediately removed from the printer.

5.3 Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.

5.4 Whiteboards containing Restricted and/or Sensitive information should be erased.

5.5 Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer

6 Policy Compliance

6.1 Compliance Measurement

It will be the responsibility of the Information Governance Group via all Corporate Managers to verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, internal and external audits, and feedback to the Information Governance Group policy owner.

6.2 Exceptions

Any exception to the policy must be approved by the Information Governance Group in advance.

6.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action.

Related Standards, Policies and Processes

- Information Governance Framework
- Data Protection Policy
- Information Security Policy
- Agile Working Policy
- Sharing Information Safely Policy

Appendix 4

Rugby Borough Council Data Protection Policy

November 2020

Document History

Version	Date	Notes	Prepared by
0.1	December 2017		Matthew Deaves
0.2	October 2020	Minor amendments for inclusion in Information Governance and Agile Working framework.	Policy Cell
0.3	November 2020	Approval by SMT	Policy Cell

Table of contents

1 Introduction

1.1 Background to the General Data Protection Regulation ('GDPR')

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

1.2 Definitions used by the organisation

Material scope (Article 2) – the GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

Territorial scope (Article 3) – the GDPR will apply to all controllers that are established in the EU who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behaviour of data subjects who are resident in the EU.

1.3 Article 4 definitions

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child – the GDPR defines a child as anyone under the age of 16 years old, although this may be lowered to 13 by the United Kingdom government. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

2 Policy Statement

2.1 The management of Rugby Borough Council, located at Town Hall, Evreux Way, Rugby CV21 2RR are committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information Rugby Borough Council collects and processes in accordance with the General Data Protection Regulation (GDPR).

2.2 Compliance with the GDPR is described by this policy and other relevant policies such as the Information Security Policy, along with connected processes and procedures.

2.3 The GDPR and this policy apply to all of Rugby Borough Council's personal data processing functions, including those performed on customers', clients', employees', suppliers' and partners' personal data, and any other personal data the organisation processes from any source.

2.4 The Data Protection Officer is responsible for reviewing the register of processing in the light of any changes to Rugby Borough Council's activities (as determined by changes to the data inventory register and the management review) and to any additional requirements identified by means of data protection impact assessments. This register will be made available on the supervisory authority's request.

2.5 This policy applies to all Employees/Councillors and interested parties of Rugby Borough Council such as outsourced suppliers. Any breach of the GDPR or this policy will be dealt with under Rugby Borough Council's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

2.6 Partners and any third parties working with or for Rugby Borough Council, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by Rugby Borough Council without having first entered into a data confidentiality agreement, which imposes on the third party obligations no less onerous than those to which Rugby Borough Council is committed, and which gives Rugby Borough Council the right to audit compliance with the agreement.

3 Responsibilities and Roles under the General Data Protection Regulation

3.1 Rugby Borough Council is a data controller under the GDPR.

3.2 Senior Management Team and all those in managerial or supervisory roles throughout Rugby Borough Council are responsible for developing and encouraging good information handling practices within Rugby Borough Council; responsibilities are set out in individual job descriptions.

3.3 The Data Protection Officer, a role specified in the GDPR, should be a senior manager. The Data Protection Officer is accountable to the Executive Director of Rugby Borough Council for the management of personal data within Rugby Borough Council and for ensuring that compliance with data protection legislation and good practice can be demonstrated.

3.4 The Communications, Consultation and Information Manager, who Senior Management Team considers to be suitably qualified and experienced, has been appointed to the role of Data Protection Officer. The Data Protection Officer will take responsibility for Rugby Borough Council's compliance with this policy on a day-to-day basis. Managers, team leaders and Heads of Service will remain responsible for all data processing that takes place within their area of responsibility.

3.5 The Data Protection Officer has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and is the first point of call for Employees/Councillors seeking clarification on any aspect of data protection compliance.

3.6 Compliance with data protection legislation is the responsibility of all Employees/Councillors of Rugby Borough Council who process personal data.

3.7 Rugby Borough Council's data protection training policy sets out specific training and awareness requirements in relation to specific roles and Employees/Councillors of Rugby Borough Council generally.

3.8 Employees/Councillors of Rugby Borough Council are responsible for ensuring that any personal data about them and supplied by them to Rugby Borough Council is accurate and up-to-date.

4 Data Protection Principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. Rugby Borough Council's policies and procedures are designed to ensure compliance with the principles.

4.1 **Personal data must be processed lawfully, fairly and transparently**
Lawful – the borough council will identify a lawful basis before processing personal data.

Fairly – the borough council will make relevant information available to data subjects in the form of a privacy notice. Privacy notices will be provided whether the personal data was obtained directly from the data subjects or from other sources.

Transparently – privacy notices will be understandable and accessible. Information will be communicated to in an intelligible form using clear and plain language.

Rugby Borough Council will provide information asset owners with clear guidance on how to produce and communicate privacy notices.

The specific information that must be provided to the data subject must, as a minimum, include:

4.1.1 the identity and the contact details of the controller and, if any, of the controller's representative;

4.1.2 the contact details of the Data Protection Officer;

4.1.3 the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

4.1.4 the period for which the personal data will be stored;

4.1.5 the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;

4.1.6 the categories of personal data concerned;

4.1.7 the recipients or categories of recipients of the personal data, where applicable;

4.1.8 where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection

afforded to the data;

4.1.9 any further information necessary to guarantee fair processing.

4.2 **Personal data can only be collected for specific, explicit and legitimate purposes**

Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of Rugby Borough Council's GDPR register of processing.

4.3 **Personal data must be adequate, relevant and limited to what is necessary for processing**

4.3.1 Information asset owners are responsible for ensuring that Rugby Borough Council does not collect information that is not strictly necessary for the purpose for which it is obtained.

4.3.2 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair processing statement or link to privacy statement and approved by the Data Protection Officer.

4.3.3 The Data Protection Officer will ensure that, on a regular basis all data collection methods are reviewed to ensure that collected data continues to be adequate, relevant and not excessive.

4.4 **Personal data must be accurate and kept up to date with every effort to erase or rectify without delay**

4.4.1 Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

4.4.2 The Data Protection Officer is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

4.4.3 It is also the responsibility of the data subject to ensure that data held by Rugby Borough Council is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

4.4.4 Employees/Councillors, residents, business owners and all other data subjects should be required to notify Rugby Borough Council of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of Rugby Borough Council to ensure that any notification regarding change of

circumstances is recorded and acted upon.

4.4.5 The Information Asset Owners are responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

4.4.6 On at least an annual basis, Information Asset Owners will review the retention dates of all the personal data processed by Rugby Borough Council, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be deleted/destroyed securely in line with any data destruction guidance that may apply.

4.4.7 The Data Protection Officer is responsible for responding to requests for rectification from data subjects. This must be completed in line with any guidance that may apply and within one month, but can be extended to a further two months for complex requests. If Rugby Borough Council decides not to comply with the request, the Data Protection Officer must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

4.4.8 The Information Asset Owner is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

4.5 **Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing**.

4.5.1 Where personal data needs to be retained beyond the processing date, it will be minimised, encrypted, anonymised, pseudonymised or otherwise protected in order to protect the identity of the data subject in the event of a data breach.

4.5.2 Personal data will be retained in line with the retention schedule and, once its retention date is passed, it must be destroyed securely in line with any data destruction guidance that may apply.

4.5.3 The Data Protection Officer must approve any data retention that exceeds the retention periods defined in the retention schedule, and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This

approval must be written.

4.6 **Personal data must be processed in a manner that ensures the appropriate security**

The Senior Information Risk Owner will carry out a risk assessment taking into account all the circumstances of Rugby Borough Council's controlling or processing operations.

In determining appropriateness, the Data Protection Officer and Senior Information Risk Owner should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or residents) if a security breach occurs, the effect of any security breach on the data subjects and Rugby Borough Council itself, and any likely reputational damage including the possible loss of trust.

When assessing appropriate technical measures, the Senior Information Risk Owner will consider the following:

- Password protection;
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media;
- Virus checking software and firewalls;
- Role-based access rights including those assigned to temporary staff;
- Encryption of devices that leave the organisation's premises such as laptops;
- Security of local and wide area networks;
- Privacy enhancing technologies such as pseudonymisation and anonymisation;
- Identifying appropriate international security standards relevant to Rugby Borough Council.

When assessing appropriate organisational measures the Data Protection Officer and Senior Information Risk Owner will consider the following:

- The appropriate training levels throughout Rugby Borough Council;
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper based records;
- Adoption of a clear desk policy;
- Storing of paper based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employee's own personal devices being used in the workplace;

- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

Rugby Borough Council's compliance with this principle is contained in its information security management system, which has been developed in line with ISO/IEC 27002.

4.7 **The controller must be able to demonstrate compliance with the GDPR's other principles** (**accountability)**

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires data controllers to demonstrate that they comply with the principles and states explicitly that this is their responsibility.

Rugby Borough Council will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans.

5 Data subjects' rights

5.1 Data subjects have the following rights regarding data processing, and the data that is recorded about them:

5.1.1 To make subject access requests regarding the nature of information held and to whom it has been disclosed.

5.1.2 To prevent processing likely to cause damage or distress.

5.1.3 To prevent processing for purposes of direct marketing.

5.1.4 To be informed about the mechanics of automated decision-taking processes that will significantly affect them.

5.1.5 To not have significant decisions that will affect them taken solely by automated process.

5.1.6 To sue for compensation if they suffer damage by any contravention of the GDPR.

5.1.7 To take action to rectify, block, erase, including the right to be

forgotten, or destroy inaccurate data.

5.1.8 To request the supervisory authority to assess whether any provision of the GDPR has been contravened.

5.1.9 To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.

5.1.10 To object to any automated profiling that is occurring without consent.

5.2 Rugby Borough Council ensures that data subjects may exercise these rights:

5.2.1 Data subjects may make data access requests as described in the Subject Access Request Procedure; this procedure also describes how Rugby Borough Council will ensure that its response to the data access request complies with the requirements of the GDPR.

5.2.2 Data subjects have the right to complain to Rugby Borough Council related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled. These complaints will be dealt with in line with the complaints procedure.

6 Consent

6.1 Rugby Borough Council understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

6.2 Rugby Borough Council understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

6.3 There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. Rugby Borough Council must be able to demonstrate that consent was obtained for the processing operation.

6.4 For sensitive data, explicit written consent of data subjects must be obtained

unless an alternative legitimate basis for processing exists.

6.5 In most instances, consent to process personal and sensitive data is obtained routinely by Rugby Borough Council using standard consent documents e.g. when signing a new contract, or during induction for participants on programmes.

6.6 Where Rugby Borough Council provides online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 13.

7 Security of data

7.1 All Employees/Councillors are responsible for ensuring that any personal data that Rugby Borough Council holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Rugby Borough Council to receive that information and has entered into a confidentiality agreement.

7.2 All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy. All personal data should be treated with the highest security and must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected in line with corporate requirements in the Access Control Policy; and/or
- stored on (removable) and encrypted storage media provided by the borough council for this purpose.

7.3 Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees/Councillors of Rugby Borough Council. All Employees/Councillors are required to enter into an Acceptable Use Agreement before they are given access to organisational information of any sort.

7.4 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit written authorisation. As soon as manual records are no longer required, they must be destroyed securely.

7.5 Personal data may only be deleted or disposed of in line with the retention schedule. Manual records that have reached their retention date are to be shredded and disposed of as ‘confidential waste’. Hard drives of redundant PCs are to be removed and immediately before disposal. If outsourced, suppliers will be treated as a data processor and a destruction certificate must be provided.

7.6 Processing of personal data ‘off-site’ presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

8 Disclosure of Data

8.1 Rugby Borough Council must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the police. All Employees/Councillors should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of Rugby Borough Council’s business.

8.2 All requests to provide data for one of these reasons must be supported by appropriate paperwork and where not part of a contract all such disclosures must be specifically authorised by the Data Protection Officer.

9 Retention and Disposal of Data

9.1 Rugby Borough Council shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

9.2 Rugby Borough Council may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

9.3 The retention period for each category of personal data will be set out in the retention schedule along with the criteria used to determine this period including any statutory obligations Rugby Borough Council has to retain the data.

9.4 Rugby Borough Council’s data retention and data disposal procedures will apply in all cases. Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the “rights and freedoms” of data subjects.

10 Data transfers

10.1 All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

The transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply:

10.1.1 **An adequacy decision**

The European Commission can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances no authorisation is required.

Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as having met the conditions for an adequacy decision.

A list of countries that currently satisfy the adequacy requirements of the Commission are published in the Official Journal of the European Union. http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

10.1.2 **Privacy Shield**

If Rugby Borough Council wishes to transfer personal data from the EU to an organisation in the United States it should check that the organisation is signed up with the Privacy Shield framework at the U.S. Department of Commerce. The obligation applying to companies under the Privacy Shield are contained in the "Privacy Principles". The US DOC is responsible for managing and administering the Privacy Shield and ensuring that companies live up to their commitments. In order to be able to certify, companies must have a privacy policy in line with the Privacy Principles e.g. use, store and further transfer the personal data according to a strong set of data protection rules and safeguards. The protection given to the personal data applies regardless of whether the personal data is related to an EU resident or not. Organisations must renew their "membership" to the Privacy Shield on an annual basis. If they do not, they can no longer receive and use personal data from the EU under that framework.

Assessment of adequacy by the data controller

In making an assessment of adequacy, the UK based exporting controller should take account of the following factors:

- the nature of the information being transferred;
- the country or territory of the origin, and final destination, of the information;
- how the information will be used and for how long;
- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
- the security measures that are to be taken as regards the data in the overseas location.

10.1.3 **Model contract clauses**

Rugby Borough Council may adopt approved model contract clauses for the transfer of data outside of the EEA. If Rugby Borough Council adopts model contract clauses approved by the Information Commissioner there is an automatic recognition of adequacy.

10.1.4 **Exceptions**

In the absence of an adequacy decision, Privacy Shield membership and/or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

11 Information asset register/data inventory

11.1 Rugby Borough Council has established a data inventory as part of its approach to address risks and opportunities throughout its GDPR compliance project. Rugby Borough Council's data inventory determines:

- business processes that use personal data;
- source of personal data;
- volume of data subjects;
- description of each item of personal data;
- processing activity;
- recipients, and potential recipients, of the personal data;
- the role of Rugby Borough Council throughout the data flow;
- key systems and repositories;
- any data transfers; and
- retention and disposal requirements.

It also maintains the inventory of data categories of personal data processed and documents the purpose(s) for which each category of personal data is used.

11.2 Rugby Borough Council is aware of any risks associated with the processing of particular types of personal data.

11.2.1 Rugby Borough Council assesses the level of risk to individuals associated with the processing of their personal data. Data protection impact assessments (DPIAs) are carried out in relation to the processing of personal data by Rugby Borough Council, and in relation to processing undertaken by other organisations on behalf of Rugby Borough Council. The method by which DPIAs are carried out will be approved in writing by the Data Protection Officer.

11.2.2 Rugby Borough Council shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

11.2.3 Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Rugby Borough Council shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.

11.2.4 Where, as a result of a DPIA it is clear that Rugby Borough Council is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as

to whether or not Rugby Borough Council may proceed must be escalated for review to the Data Protection Officer.

11.2.5 The Data Protection Officer shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority.

11.2.6 Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to Rugby Borough Council's current risk appetite and the requirements of the GDPR.

Appendix 5

Rugby Borough Council Sharing Information safely - Anonymisation and pseudonymisation policy

November 2020

Document History

Version	Date	Notes	Prepared by
0.1	23/07/2019	First draft	Jeremy Carter
0.2	18/09/2020	Final draft	Policy Cell
0.3	23/11/2020	Approval by SMT	Policy Cell

Table of contents

1 Introduction

1.1 The Data Protection Act 2018 and General Data Protection Regulation (GDPR) requires us to use the minimum personal data necessary for a purpose. Secondary uses of personal information must not breach our obligations of confidentiality and respect for private and family life. This guidance identifies how we will use anonymisation and pseudonymisation to share information safely. This includes the use of storyboards for training and publicity purposes and the presentation and publication of statistics relating to individuals.

1.2 Anonymisation and pseudonymisation enables the Council to undertake secondary use of personal data in a safe, secure and legal way.

1.3 We share and publish information in order to undertake our functions as a Council. Through a number of channels we collect customer information such as name, address, and date of birth. However, if we remove these identifiable details, information can then be used for secondary purposes without fear of breaching the General Data Protection Regulation.

1.4 This process is called anonymisation. By removing the personal information, it allows the Council to share or publish more data with fewer restrictions.

2 Purpose

2.1 The purpose of this policy is to ensure a standardised approach to enable consistency throughout the Council, with regard to how and when to anonymise information correctly.

2.2 This policy is part of the Council's suite of Information Governance policies.

3 Scope

3.1 This policy extends to all employees of the Council who process information on its behalf.

3.2 All must comply with this policy where anonymised information is to be produced or published from individual level data.

3.3 This policy does not cover the use of information sharing agreements (if in place), or other tools used to share personal data safely. For further information on information sharing agreements please refer to the Information Governance Framework.

4 What is Anonymisation and Pseudonymisation?

4.1 Anonymisation and pseudonymisation both relate to the concealment of an individual's identity.

4.2 Anonymisation is the process of removing, replacing and / or altering any identifiable information (identifiers) that can point to the person(s) it relates to.

4.3 Pseudonymisation is the technical process of replacing the identifying information to protect the individual's identity whilst allowing the recipients to link different pieces of information together. A nickname is an example of pseudonymisation, although other identifying information such as age, ethnicity, gender or specific medical condition may also be changed to prevent a person being identified.

5 Definitions

5.1 Personal Identifiable Information (PII) is any information that can identify an individual. This could be one piece of information, or a collection of information, for example a name, address and date of birth.

5.2 Primary use refers to the use of information for the purpose of delivering Council services to individuals. This also includes relevant supporting administrative processes and audit/assurance of the quality of services provided. Primary use requires information at the person identifiable level.

5.3 Secondary use refers to the use of information about individuals for research purposes, audits, service management, commissioning, and contract monitoring and reporting. When PII is used for secondary uses the information should, where appropriate be limited and de-identified so that the secondary use process does not enable individuals to be identified.

5.4 Anonymisation is a term for a variety of statistical and other techniques that depersonalise information about people so that the specific data subjects cannot be identified, including via aggregation and pseudonymisation.

5.5 Aggregation is an anonymisation technique in which information is only presented as totals, so that no information identifying individuals are shown. Small numbers in total are a risk here and may need to be omitted or 'blurred' through random addition and subtraction.

5.6 Pseudonymisation is the de-identification of individual level information by attaching a coded reference or pseudonym to each record. This allows the information to be associated with a particular individual without the individual being otherwise identified. If the same system of pseudonyms is used across different datasets, then these datasets can be combined for analytical purposes without revealing the

identities of individuals. Again, care needs to be taken if combining datasets, for example those which could lead to individuals being identifiable via a combination of their circumstances.

5.7 Re-identification or de-anonymisation is where anonymised information is turned back into personal information, for example through the use of data matching or combining. Where anonymisation is being undertaken, the process must be designed to minimize the risk of re-identification.

6 Why Anonymise

6.1 Anonymisation is undertaken to protect the privacy of individuals, whilst still making data available for statistical or analytical purposes. Personal data does have to be used directly where the intention is to inform decisions about particular individuals, or to provide services to them. Where this information is not needed at this level and for these purposes, however, it should be anonymised.

6.2 The GDPR is concerned with 'personal data' which relates to living individuals who can be identified from such data. Anonymised data where the prospect of identifying individuals is remote is not seen as personal data. The GDPR is therefore not applicable.

7 Benefits of Anonymisation

7.1 All organisations that process personal information are required by the GDPR to protect it from inappropriate disclosure.

7.2 Where the Council wants to or is required to publish information derived from such personal information, for example for analytical or statistical purposes, anonymisation techniques enable this information to be made available to the public and others without revealing any personal identifiable information. This ensures compliance with Data Protection obligations.

8 Risk of Re-identification of Anonymised Information

8.1 When anonymising information, the Council must be sure that the information is assessed, and the risks mitigated. This includes assessing whether other information is available that is likely to facilitate re-identification of the anonymised information.

8.2 The GDPR states that personal information is information which relates to a living individual who can be identified from that information, or from information which is in the possession of, or is likely to come into the possession of, the data controller.

8.3 When assessing whether information has been anonymised effectively, it is necessary to consider whether other information is available that, in combination with the anonymised information, would result in a disclosure of personal information. This is most likely where the circumstances described by the combined information are unusual or where population sizes are small.

8.4 Anyone considering anonymisation should carry out a 'motivated intruder' test, recommended by the Information Commissioner's Office as a means to check whether information has been effectively anonymised. This checks whether a reasonably competent individual who wished to de-anonymise information could successfully do so. The test involves finding out whether information in the anonymised dataset could be combined with searches of easily available information to reveal the identity of individuals. Examples might include the electoral register, social media, press archives or local library resources.

8.5 Issues to consider are as follows:

- What is the risk of a 'jigsaw attack', piecing different items of information together to create a more complete picture of someone? Does the information have characteristics which facilitate information linkage?
- What other 'linkable' information is easily available?
- What technical measures might be used to achieve re-identification?
- What re-identification vulnerabilities did the motivated intruder test reveal?
- How much weight should be given to individuals' personal knowledge?

8.6 Re-identification would lead to the unintentional disclosure of personal or sensitive personal information and would therefore be an information security incident. This should be reported as soon as possible using the Council's information security incident process.

9 Anonymisation / De-identification

9.1 Staff should only have access to the information that is necessary for the completion of the business activity they are involved in. This principle applies to the use of PII for secondary or non-direct purposes. Through de-identification, users are able to make use of individual information for a range of secondary purposes without having to access the identifiable information items.

9.2 The aim of de-identification or anonymisation is to obscure the identifiable information items within the person's records sufficiently so that the risk of potential

identification of the information subject is minimized to acceptable levels: this will provide effective anonymisation.

9.3 De-identification can be achieved via a range of techniques. Whether de-identification is achieved depends on the fit of the technique with the specific dataset. Techniques include:

- Aggregation so that information is only viewed as totals.
- Removing person identifiers.
- Using identifier ranges, for example: age ranges instead of age, full or partial postcode instead of full address, or age at activity event instead of date of birth.
- Using pseudonyms.

9.4 De-identified information that goes down to the level of the individual should still be used within a secure environment with staff access on a need to know basis.

10 Pseudonymisation

10.1 When pseudonymisation techniques are consistently applied, the same pseudonym is provided for individuals across different datasets and over time. This allows datasets and other information to be linked in ways that would not be possible if person identifiable information was removed completely.

10.2 To effectively pseudonymise information, the following actions must be taken:

- Each field of PII must have a unique pseudonym;
- Pseudonyms to be used in place of personal data and similar fields must be of the same length and formatted on output to ensure readability. For example, in order to replace a surname in existing report formats, the output pseudonym should generally be of the same field length, but not of the same characters.
- Other identifiable fields should be replaced by alternatives which render the information less specific (e.g. age at activity event replacing date of birth, lower super output area replacing postcode).
- It should be clear from the format of pseudonym information that it is not ‘real’ information to avoid confusion, e.g. adding numbers that would not ordinarily appear in a surname.
- Consideration needs to be given to the impact on existing systems, both in terms of the maintenance of internal values and the formatting of reports.

Related Documents

- Data sharing agreements (Where in place)
- Information Security Policy
- Data Protection Policy
- Information Governance Framework
- Clean Desk Policy

Appendix 6

Rugby Borough Council Information Security Policy

November 2020

Document History

Version	Date	Notes	Prepared by
0.1	27/09/2019	First draft	Jeremy Carter
0.2	24/09/2020	Final draft	Policy Cell
0.3	23/11/2020	Approval by SMT	Policy Cell

Table of contents

1 Introduction

1.1 Rugby Borough Council (the Council) exists in an ever-changing technological world and to ensure we can continue to operate in this environment and continue to do business we must be more aware of security issues and measures that protect the Council's key assets, defined by:

- Its people
- Its business (products and services)
- Its infrastructure to support the business
- Its information

1.2 Security attacks against Local Authorities like Rugby Borough Council are increasing all the time and we must ensure our systems can be protected against these threats. By complying with the rules and guidelines articulated in this policy, we are doing everything we can to protect our systems and our people from a security threat. Most of the requirements in this policy are based on published standards and you are required to understand your obligations.

2 Purpose

2.1 This Information Security Policy establishes effective controls for the protection of information owned, maintained or entrusted to the Council. This policy is aligned with the Council's overarching system of ICT Standards and Procedures that lays the foundation for best practices in security management and ongoing compliance with the Council's regulatory and legal obligations. For further information or clarification regarding any of the Council's policies or procedures logon to MetaCompliance.

3 Objective

3.1 The Council is committed to ensuring that:

- Information is protected against unauthorised access.
- Confidentiality of information is maintained.
- Information is not disclosed to unauthorised persons through deliberate or careless action.
- The integrity of information is protected from accidental or unauthorised modification.
- Information is available to authorised users when needed.

- Regulatory and legislative requirements are met.
- Business continuity and systems recovery plans are produced, maintained, and tested as far as practicable; and
- All breaches of information security and suspected weaknesses are reported and investigated.

This will be achieved by:

- Identifying through appropriate and regular risk assessment any vulnerabilities and/or threats that may expose the Council's information assets to risk, and
- Ensuring that all applications containing financial, critical, private, or confidential information are password protected, and
- Managing the risks to an acceptable level through the design, implementation and maintenance of appropriate procedures and standards.

4 Scope

4.1 Information security is all about keeping corporate information safe. This policy addresses the need to protect confidential and sensitive information from disclosure, unauthorised access, loss, corruption and interference and is relevant in both electronic and physical formats. Security can be defined by three things:

Confidentiality: information must not be made available or disclosed to people other than employees that need access to that information to carry out their Council duties.

Integrity: data must not be altered or destroyed in an unauthorised manner, and accuracy and consistency must be preserved regardless of changes.

Availability: information must be accessible and useable on demand by people that need to access that information to carry out council duties.

4.2 A holistic approach to security encompasses the following areas:

- Information security
- Communications security
- Technical security
- Computer security
- Personnel security
- Physical security

5 Applicability and Definitions

5.1 This policy applies to all Council employees, members, contractors, and where applicable, suppliers and other third parties, hereby after referred to as “users”.

6 Policy Statements

6.1 The policy statements included in this document are intended to provide guidance for users, and to support interpretation of the policy. Any statements contained within this policy should be read as requirements of the Employee Code of Conduct.

6.2 **Intellectual Property**

All information created, sent, received or processed during Council business is owned by the Council, unless the information is subject to the intellectual property rights of other parties.

6.3 **GDPR**

The General Data Protection Regulation and other relevant legislation apply, and in that context Council employees are obligated to protect and handle information in accordance with privacy and confidentiality principles. Subject to those provisions, Council employees have the right to access, review, monitor, and disclose information to:

- Ensure information processing systems are used appropriately.
- Ensure the protection of information assets; and
- Ensure that legal responsibilities are met.

All users must be aware of the need to protect records and information from inappropriate and/or unlawful disclosure, and that the Council’s management and staff have a duty of care to ensure the safe keeping of all information under its control.

6.4 **Confidentiality**

All information collected or maintained by the Council is considered restricted unless specifically classified otherwise and must not be disclosed to any unauthorised person. All users must comply with any and all relevant legislation when dealing with Council information, including the General Data Protection Regulation, Data Protection Act 2018, the Freedom of Information Act, the Public Records Act, and the Local Government Act.

6.5 **Access Control**

6.5.1 Users are only permitted to access information, applications, and systems that they have been allocated access rights for. Rights are granted based on

business need and documented in an access control statement that defines the rules and rights for individuals or groups. Any other access is considered unauthorised and is in breach of this requirement.

6.5.2 Mobile phones, tablets, portable computers, laptops, USB devices or any other device must not be connected to Council's internal computer systems or networks unless the appropriate access controls have been installed and the device has been approved for such use by the Corporate ICT Manager.

6.5.3 Damaging, altering, or disrupting the operations of the computer systems and networks owned or managed by Council is not permitted. Users must not carry out any activity with the intention of capturing or obtaining passwords, encryption keys, or anything that could facilitate unauthorised access by themselves or anyone else.

6.5.4 Before a user reaches a menu, system prompt or has access to system utilities, databases or shares they must have successfully logged on and be validated as a legitimate system user. Authentication methods including single sign on will depend on the sensitivity of the information or system being accessed, whether access is affected in-house or remotely and the level of privileges granted to the user.

6.6 Antivirus

6.6.1 Users must not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise affect the performance of, or access to any Council computer system or network.

6.7 Business Continuity/Disaster Recovery (DR)

6.7.1 Users of computer systems and networks owned or managed by Council must notify management as soon as possible of any condition that could lead to a disruption of normal business activities. Examples include:

- ineffective security controls
- issues relating to information integrity, confidentiality or availability
- human errors
- non-compliance with Standards or Guidelines
- breaches of physical security arrangements

- uncontrolled system changes
- access violations
- weaknesses in security or potential security vulnerabilities
- system malfunctions
- missing files
- potential hazards in the workplace such as electrical wiring hazards

6.8 Communication and Mobile Devices

6.8.1 Mobile devices and communication systems supplied by the Council are provided to facilitate business activities. Reasonable and appropriate personal use is permitted as follows:

- Minimal calls and text messages
- The data plan must not be exceeded due to personal use
- Personal use must not cause the Council to incur any additional costs or impact user productivity

6.8.2 Service managers will monitor use and are provided with monthly reports. Excessive personal use may be required to be reimbursed by the employee.

6.8.3 A phone or smartphone supplied by Council may not be used in connection with any personal commercial business activities. The number may not be published in any publication or business card that is not related to the Council's business.

6.8.4 Mobile devices and communication systems owned or managed by Council are to be used in an effective, safe, ethical and lawful manner. Use will be monitored, and misuse will be handled in accordance with existing disciplinary procedures.

6.8.5 Users of Council mobile phones and communication systems must not engage in any activity which violates or infringes the rights of others or which a reasonable person would consider to be abusive, profane, offensive or defamatory. This requirement protects against breaches of human rights legislation.

6.8.6 Communications equipment supplied by Council must not be altered or added to in any way including:

- unauthorised upgrades
- addition of components
- removal of components - including transferring a Council SIM card to a personal device

- altering configuration or security settings
- jailbreaking the device

6.8.7 All devices will be centrally managed (via a corporate mobile device management system) and any changes or maintenance carried out by the IT Service Desk or designated officer.

6.8.8 Users of mobile devices must ensure that the device is protected by a PIN number or password and auto-lock. Voice authentication (if used), must be coupled with password or PIN authentication.

6.8.9 The Council maintains the right to conduct inspections of any mobile phone or other mobile device that it owns or manages without prior notice to the user or custodian. The device must be returned to the IT Service Desk upon request for maintenance, updates, and when the user ceases to provide services to Council.

6.8.10 Users should not lend mobile devices allocated to them for business activities to others external to the Council including friends and family.

6.8.11 Users of communications devices must not return calls, text messages, respond to pager calls or subscribe to paid services where:

- charges beyond those for normal calls can be incurred (e.g. long-distance calls, payed services)
- the recipient is a competition, gambling or advertising entity
- charges will be reversed back to the Council

Any costs incurred relating to the above will be the responsibility of the employee and such expenditure may be deducted from salary

6.8.12 With the exception of purchases made from an approved online application store (e.g. the Council's Application Store, games, freeware, shareware, movie clips or music may not be downloaded onto any Council mobile device unless its use is legal (does not breach copyright law) and it is specifically required for business purposes. Movie clips taken with the device for work purposes are exempt from this requirement.

6.8.13 Personally, owned communication devices may not be connected to or synchronised with Council's computer systems or networks unless approved by the Corporate ICT Manager and the device owner agrees to the security requirements regarding the management of the device. Bring Your Own Device (BYOD) users must agree:

- That the device will be managed by Council's device management system; and
- That the Council security profile is applied to the device.

6.8.14 The use of non-corporate voice and video communication accounts must be approved by the Corporate ICT Manager. Voice and video systems are not to be used for any of the following:

- personal voice calling, video calling and instant messaging
- commercial announcements
- advertising material
- sexually explicit or sexually oriented material
- hate based material
- hacker related material
- transferring of files
- All inbound and outbound communication must be channelled through corporate systems and accounts.

6.9 Computer Systems and Equipment Use

6.9.1 Users of computer systems or networks owned or managed by Council shall not use these systems to engage in any activity which causes, or could be construed as causing, any form of harassment, discrimination or victimisation of another person including:

- Race
- Religious belief or activity
- Sex
- Age
- Disability
- Industrial association
- Lawful sexual activity/sexual orientation
- Marital, parental or carer status
- Physical features
- Political beliefs or activity
- Personal association with a person who has one of these personal characteristics
- Gender
- Irrelevant criminal conviction

6.9.2 The computer systems and networks owned or managed by Council are to be used in an effective, safe, ethical and lawful manner, and in compliance with the Council's existing IT policies. Misuse of ICT resources may lead to disciplinary proceedings.

6.9.3 The computer systems are to be used for business purposes in the course of normal day to day operations. Personal use must be reasonable and appropriate

and not impact on user productivity, system performance or bring the Council into disrepute.

6.9.4 Users must not connect personally owned computing devices, computer peripherals, USB devices, digital cameras etc. to computer systems or networks owned or managed by the Council unless compliant with the BYOD section. If users do bring personal equipment to work, this is at their own risk and the Council is not responsible for the device or anything stored on it.

6.9.5 Computer equipment supplied by Council must not be altered or added to in any way including:

- unauthorised upgrades
- addition of components
- removal of components
- altering configuration or security settings
- installation of non-approved applications
- All changes to configuration or maintenance of the device must be carried out by ICT staff or their designated agent.

6.9.6 Users must not lend computers, portable devices, tablets, mobile phones, laptops or any other equipment that has been allocated to them by the Council for business activities to anyone external to the Council including friends and family.

6.9.7 Users must use the standard applications for which the Council is licensed. Do not install any software program, application, script or executable code on equipment in your care. Only software approved by the ICT Department may be installed on computer equipment owned by Council and all installations must be carried out by ICT staff.

6.10 Cyber Crime and Security Incidents

6.10.1 Any actions or activities, whether intended or accidental which cause, or could cause the computer systems, information or networks to be compromised in any way is considered serious misconduct including:

- Security breaches or disruptions of network communications.
- Port scanning or security scanning. These activities are expressly prohibited unless sanctioned by the Corporate ICT Manager for the purposes of testing network security.
- Executing any form of network monitoring which will intercept data not

intended for the employee's host, unless this activity is a part of the employee's normal duties or has been duly authorised.

- Circumventing user authentication or security of any host, network or account or running password cracking programs.
- Interfering with, or denying service to other users (for example, denial of service attack).
- Using any program, script, command, or sending messages of any kind, with the intent of interfering with or disabling a user's session using any means either locally or externally.
- Downloading, installing or executing any file containing malware which may damage or compromise computer systems or data.
- Copying or altering configuration or system files for unauthorised personal use or to provide to other people or users for unauthorised use.
- Creating or using open mail relays maliciously, spoofing mail headers, initiating a mail bomb attack or otherwise interfering with the Council's or another organisation's email service.
- Downloading or introducing tools or utilities that may potentially be used for hacking activities and undertaking any such activity on any system whether owned or managed by the Council or not.
- Providing or selling the Council's information without approval and for personal gain.
- Defacing websites, downloading and distributing pornography, running a gambling operation or undertaking any other activity using the Council's resources that would bring the Council into disrepute.

6.11 Email

6.11.1 The email system is predominantly for business use. Personal use must be reasonable and appropriate and not impact on user productivity, system performance or bring Council into disrepute. Misuse will be handled in accordance with existing Council disciplinary procedures.

6.11.2 The email system must not be used for any unlawful activity and must not be used to compromise the security or operation of any computer system or network whether it is owned or managed by Council or not.

6.11.3 Users must not create, send or forward any email messages which contravene

human rights legislation, and which may be considered discriminatory, defamatory, intend harassment or hatred on the basis of:

- Race
- Religious Belief or Activity
- Sex/ gender
- Age
- Disability
- Industrial Association
- Lawful Sexual Activity/Sexual Orientation
- Marital, Parental or Carer Status
- Physical Features
- Political Beliefs or Activity
- Personal Association with a person who has one of these personal characteristics
- Irrelevant criminal conviction

Misuse will be handled in accordance with the Council's disciplinary procedures.

6.11.4 The email system is regarded as an official means of communication and, as such, messages must conform to the same corporate rules for grammar and content as other business communications. It is not appropriate to use abbreviations (as used in text messages) or profanities, obscenities, derogatory or sexually explicit remarks in business email messages. Such remarks, even when made as a joke, may upset some people. Special caution is warranted because backup and archival copies of email may be more permanent and more readily accessed than traditional paper communications.

6.11.5 Sending or receiving email with another user's account or reading another user's email is prohibited. If there is need to read another's mail (e.g. while they are away) message forwarding or delegated authority functions must be initiated by the owner of the email account and rescinded when no longer required.

6.11.6 Distribution groups are to be created and maintained by the Information Technology Department. New distribution groups will only be added by using the correct process of contacting the Service Desk Team via the Service Desk portal. The requested group will then be authorised by one of the IT Lead Officers The person responsible for the group must inform the Service Desk of any changes to group membership in a timely manner and is responsible for regularly checking that group membership is valid.

6.11.7 The email system is the property of Council and all messages sent or received by it, or stored within it, are owned by the Council. The Council reserves the right to access and disclose all messages sent and received over its email system if required by law or valid business purpose providing permission has been granted

by the relevant Head of Service.

6.12 **Information Management**

6.12.1 Data and information created modified saved, transmitted or archived using the corporate systems of Council remains the property of the Council.

6.12.2 All corporate information and data must be stored in approved corporate information repositories. This includes Information@Work SharePoint, corporate applications and other approved shared repositories. Information is not to be stored in Outlook mailboxes or on local drives of PCs or workstations, laptops or copied onto portable media such as CDs or DVDs unless these copies are made in addition to saving it in an approved corporate information repository.

6.12.2(a) Corporate information is defined as any information that documents or supports the administrative, financial, legal and business transactions and functions of the Council. Corporate information can be both electronic and hard copy. Emails, audio and video recording, documents, social media postings, plans and images are all examples of electronic corporate information.

6.12.3 Electronic information must be protected based on its sensitivity, value and criticality regardless of the type of media that holds the information, its location, the systems used to process it or the processes it is subjected to.

6.12.4 The user must report a breach or near miss incident immediately if confidential or sensitive information is lost, disclosed to unauthorised parties, or is suspected of being lost or disclosed.

6.12.5 Users must not delete or dispose of potentially important Council electronic records or information without the approval of the information owner and without following standard document management procedures for disposing of information. Deleting the Council's records without following the proper procedures is considered a serious breach of this requirement particularly if the records cannot be recovered. and could potentially lead to disciplinary action.

6.13 **Encryption Use**

6.13.1 Encryption must be used to protect data where the risk of loss through theft or interception is high, where there is the potential for a major security breach should that data get into the hands of unauthorised persons and where the loss of the data would have a major impact on the Council's reputation or business.

6.13.2 Data which is classified as confidential or sensitive must be protected from unauthorised access. This includes data stored on mobile devices, USB sticks and laptops, data accessible via network shares, system files (e.g. those that contain passwords) and information transmitted over the internet or other public network (e.g. email).

6.14 Protection of Hardcopy Material

6.14.1 Storing hard copy material is discouraged as much as possible. Utilising digital ways of working is strongly encouraged but if hard copy information is stored then its protection is imperative due to the risk of improper disclosure or loss. Measures for the protection of such paper records must comply with the Public Records Act and the Council's information management policies.

6.14.2 All paper records must be retained or disposed of in accordance with relevant legislation and/ or Council policy.

6.14.3 Destruction of any confidential records must be done in a secure manner, using the destruction bins available.

6.14.4 No confidential material should be left in an unsecured work area, or any location directly accessible by the public.

6.15 Internet Use

6.15.1 The internet is primarily available for business use. Personal use must be reasonable and appropriate, carried out in employees' own time, not impact on user productivity or system performance, or bring Council into disrepute. A web content control system monitors and controls website visits. The Council monitors and logs web sites visited, files downloaded, and social networking accounts controlled by the Council. Line managers and heads of service can request reports that allow them to monitor and moderate internet use. Users viewing or downloading content that is deemed inappropriate for the workplace may be subject to disciplinary actions up to and including dismissal.

6.15.2 Users of the internet are not permitted to visit, interact with, or download content from websites that are offensive, obscene or contain indecent material such as pornography or violence. Users must not access, publish or download material which promotes hatred or discrimination based on:

- Race
- Religious Belief or Activity
- Sex/ gender
- Age
- Disability
- Industrial Association
- Lawful Sexual Activity/Sexual Orientation
- Marital, Parental or Carer Status
- Physical Features
- Political Beliefs or Activity
- Personal Association with a person who has one of these personal characteristics
- Gender
- Irrelevant criminal conviction

The above activities should be reported to your Line Manager or Human Resources. All reports will be investigated and handled in accordance with existing disciplinary procedures.

6.15.3 The internet connection must not be used for any illegal or unethical activity or personal business activity and must not be used to compromise the security of any computer system or network whether owned or managed by the Council or not. Misuse must be reported to a Head of Service or Line Manager, Human Resources or the Information Technology team immediately. Reports of misuse will be investigated and handled in accordance with the Council's disciplinary procedures. Examples of unacceptable internet use include:

- computer hacking (accessing another's electronic data or computer without permission)
- providing access to unauthorised persons (including minors)
- impersonation
- file downloads (except for work related reasons)
- use of the internet for personal gain
- gaming, wagering or betting
- the intentional transmission in any way of viruses or files that cause a negative impact on computer systems (e.g. unauthorised email attachments such as video, audio and executable files)
- downloading or distributing information subject to copyright requirements (such as licensed software or protected internet applications)
- disclosing private or confidential information including passwords or other

information that may compromise the security of the computer systems

- engaging in any illegal activity, including dissemination of material in breach of legislation

6.15.4 Peer to peer sharing of personal files is not permitted. This requirement includes sharing or downloading of movies, music, eBooks, applications, games etc using torrent sharing, torrent clients and file sharing connections.

6.15.5 When working on their desktop within the Council's premises, users must use the internet connection provided from this equipment. Users must not circumvent internet security by using USB modems, personal hotspots, USB mobile wireless devices and mobile broadband cards. These alternative methods of connecting to the internet will be allocated to users working remotely and the Corporate ICT team will record all instances where alternative methods of connecting to the internet have been provided.

6.15.6 The internet shall not be accessed from another employee's PC/Laptop/Device unless the user is logged on with their own username and password.

6.15.7 Internet access to social media web services for personal use is permitted only in employees' non-working time. This requirement includes:

- Social networking sites including Facebook, Twitter, SnapChat, TikTok etc
- Video and photo sharing sites including YouTube, Flickr
- Collaborative information sites including Wikipedia
- Social news sites
- Access to social media is only permitted in accordance with the Social Media Policy.

6.15.8 Users must not use social media to cause annoyance or anxiety, to harass, to defame or to transmit unsolicited commercial or advertising material. These actions must be reported to a member of the senior management team or Human Resources and will be handled in accordance with existing disciplinary procedures.

6.15.9 Employees are not permitted to create or maintain an external or public facing blog, wiki or social networking site on behalf of the Council without the express permission of the Executive Director. The creation or maintenance of an internally facing blog, wiki or social networking site requires manager approval. Any blog,

wiki or shared workspace must have a moderator and an approved code of conduct.

6.16 **Legal Compliance**

6.16.1 Users must not disclose any confidential information belonging to the Council or otherwise coming into their possession during the course of their employment, except as expressly permitted under any of the Council's policies or as required by law. Users may be required to sign a confidentiality or non-disclosure agreement. Information may be classified as follows (further information can be found at Appendix A):

- **Not to be Stored**: Information which may not be captured or saved in electronic systems
- **Confidential**: Information restricted to a small number of people
- **Restricted (Internal Use Only)**: Information which may be known by users, but not by anyone external to the Council
- **Public**:\ Information that is approved for public dissemination.

6.16.2 Users will often disclose information during the normal course of their duties and may be legally required to disclose information upon request. However, information that, by its nature, is confidential, must not be disclosed except as expressly permitted under any of the Council's Standards or as required by law (e.g. under Privacy or Freedom of Information legislation). Unauthorised disclosure of confidential information may constitute misconduct or serious misconduct. This includes disclosure using email, internet, social media, bulletin boards, list servers or printing, photocopying and/or distributing the physical document.

6.16.3 All intellectual property (including patents, copyrights, trademarks, logos, designs, inventions or other intellectual property) created and/or developed by the Council's employees while at work or while using the Council's equipment is the exclusive property of the Council.

6.16.4 Third party software in the possession of the Council must not be copied or installed multiple times unless this is allowed by the license agreement. In all other cases the number of installations should be equal to the number of licenses held. Systems will be monitored to ensure software license conditions are being complied with and license numbers are not being exceeded.

6.16.5 Information held in all computer systems and networks owned or managed by the

Council is subject to the provisions of GDPR legislation and users should be aware of their obligations in respect of managing and using the information and providing information to third parties.

6.17 **Online (Cloud) Services**

6.17.1 When using the Council's computer systems, or when conducting the Council's business, users must not deliberately misrepresent themselves and, where possible, provide full contact details.

6.17.2 Unless approval has been obtained in advance from the Senior Management Team, users are prohibited from establishing online business to business arrangements or signing up to online (cloud) services provided via the internet. Where the online system involves payments or receipts, a secure platform for processing transactions must be approved. Examples include electronic purchasing, personnel management systems, on-line database services, Sharefile, iCloud, Skype etc. Requests for a new computing initiative should be made on the IT Service Desk

6.17.3 Users must not publish corporate information (applications, internal documents or files, press releases, price lists etc.) on any public facing computer system (e.g. website, social media site) unless the item has been authorised by the appropriate manager and the Communication, Consultation and Information Manager.

6.17.4 Financial transactions transacted online must comply with legal requirements, be within approved limits of delegated authority for expenditure and meet the requirements of the Council's external auditors.

6.18 **Password and Authentication**

6.18.1 User IDs and passwords must not be disclosed to anyone or shared with anyone.

6.18.2 Group or generic User IDs and passwords are prohibited as a rule, but in special circumstances may be approved by the Corporate ICT Manager who will keep a record of the exceptions.

6.18.3 Passwords are a common way to verify an identity. It is important that the password for your network user-id cannot be easily guessed.

6.18.4 All network user passwords will expire after 180 days. User must observe the following with respect to network user-id and password requirements:

- Passwords must have a minimum length of 10 characters;
- To satisfy complexity rules, passwords must use at least three of the four available character types:
  - Lowercase letters
  - Uppercase letters
  - Numbers
  - Symbols

- You cannot re-use any of your last 3 passwords;
- Your password must not be a common word; and
- Your password must not contain your network user-id, either forwards or backwards

6.18.5 The above password policy must be applied (where practicable) to external cloud-based software accounts.

6.18.6 Passwords must not be written down and left in a place where unauthorised persons might discover them.

6.18.7 Users are responsible for all activity performed with their personal user IDs and passwords. Users must not allow others to perform any activity with their user IDs and are not permitted to perform any activity with IDs belonging to other users.

6.19 Personnel Management

6.19.1 Employees must avoid actual or potential conflicts of interest in their capacity as an employee and conducting business on behalf of the Council and if there is any doubt about a particular situation, they should consult their Manager and complete a Declaration of Interests Form.

6.19.2 All users of Council's computer systems must agree to comply with this policy and sign the Information Security User Agreement.

6.19.3 When employment ceases or a contract is completed employees, contractors, consultants, agency workers, casuals and temporary employees must hand back anything other than that which is considered personal property. This may include material or information that was provided or created during employment and equipment or property belonging to Council.

6.20 Physical Access

6.20.1 Visitors or other third parties requiring access to the Council's computer facilities must be accompanied by an authorised staff member. Photographic, video, audio or other recording equipment such as cameras in mobile devices should not be allowed in a restricted area (such as the server room) unless authorised. Visitors, contractors and other third parties must not be permitted to use employee entrances or other uncontrolled access leading to restricted areas.

6.20.2 Visitors must sign in at the reception area prior to gaining access to any restricted computer areas. Visitors must wear identification and be admitted only for legitimate purposes by authorised staff. Visitor identification must be returned, and the visitor sign out prior to leaving. Visitor access must be in accordance with any applicable Occupational Health and Safety requirements.

6.20.3 Monitor for unauthorised persons following you through secure access doors. This is called ‘tail- gating’ and is a common practice for unauthorised persons attempting to gain access. ‘Unauthorised persons’ may include Council employees who are not authorised to access a particular location at the time access is sought.

6.20.4 Server rooms and other restricted areas are monitored by security cameras. The cameras should be configured to record if they detect movement inside the area. Where security cameras are not installed in server rooms, an authorised staff member must remain inside the room whenever the doors are open or external parties are in attendance.

6.20.5 Workstations, computers, laptops and other devices used to perform the Council's business activities, irrespective of where they are located, must be protected by a password. When a user leaves their computer they must lock the screen.

6.20.6 Confidential or sensitive information displayed on the screens of computers or mobile devices must always be protected from unauthorised disclosure this includes when working away from Council offices or sites, for example working at home. Screens must be positioned, wherever possible, so that they cannot be viewed by looking over the shoulder of the person using the device or by looking through an office window. Privacy screens may be required for screens that others can easily view.

6.20.7 Identification badges, physical access cards and computer authentication tokens that have been lost or stolen or are suspected of being lost or stolen, must be reported to Facilities or the IT Service Desk immediately so that they can be cancelled.

7 Responsibilities

7.1 The Senior Management Team is responsible for approval and authorisation of this policy, and for the granting of exemptions.

7.2 The Corporate ICT Manager is responsible for:

- The provision and implementation of assets, supporting systems, applications and processes that give effect to this policy, and
- The establishment and maintenance of monitoring and compliance systems and processes to ensure that the supporting mechanisms function effectively
- The development and conduct of training sessions as required.

7.3 Managers and Lead Officers are accountable for the proper induction of new users, including permanent, fixed term employees, agency workers and casuals and for ensuring that all users in their area are made aware of this policy and the consequences of breaching it. They are also accountable for ensuring that their staff members attend and complete any compulsory IT training sessions as may be offered from time to time.

7.4 All users must read and acknowledge their understanding of this policy in order to receive credentials for accessing the Council's information systems.

7.5 All users are required to follow the directives outlined in this policy. In addition, all users have a responsibility for reporting security incidents and any identified weaknesses to the IT Service Desk.

8 Exemptions

8.1 Exemptions to this policy require the approval of the Senior Management Team.

9 Policy Breach

9.1 Instances of non-compliance with this policy will be regarded as misconduct and will be acted upon in line with the Council's disciplinary policies and procedures.

9.2 Actions for dealing with non-compliance may include further education and training, counselling, issuing of warnings, suspension of access rights, termination of contractual agreements, termination of employment, and/or legal proceedings.

10 Information Security User Agreement

I,_____,

have been provided with a copy of Rugby Borough Council's *Information Security Policy*.

I have read this document and acknowledge that I understand its contents and the obligations that it confers to me as a user of the Council's information resources.

In addition, I agree to comply with the policy and the directives contained within it.

If I have access to and use of a Council provided mobile device, e.g. smart device, laptop etc., I also acknowledge that my use of that device will at all times be in accordance with this policy.

Signature: _____

Title: _____

Date: _____

Contractor: Yes / No

Note:
A signed copy of this page must be forwarded to the Human Resources department for processing. The user must keep the remainder of the policy document for reference.

Log-on credentials will not be provided to new users until the IT Service Desk receives confirmation from the Human Resources department that a signed agreement has been received.

Appendix A

Information is classified using the following scales with regard to its 'confidentiality'.

Security Level	Description
Confidential	The data being available on an authorised need-to-know basis only (confidential and limited access) Compromise could cause limited damage to the Council, its clients, commercial entities or other members of the public, including: • Breaches of client confidentiality • Cause substantial distress to clients, other individuals or private entities • Cause financial loss or loss of earning potential to, or facilitate improper gain or advance for, individuals or private entities • Prejudice the investigation or facilitate the commission of crime • Breach proper undertakings to maintain the confidentiality of information provided by third parties • Impede the effective development or operation of Council policies • Breach other statutory restrictions on the management and disclosure of information • Disadvantage the Council in commercial or policy negotiations with other parties.
Restricted (Internal use only)	The data being openly available to the Council's personnel only, and perhaps fee-for-service public information (restricted and internal use)
Public	No requirement for confidentiality. This might be the case for certain free- of-charge public information services, Council business and commercial publications not considered copyright or commercial-in-confidence.
Not to be Stored	Information which may not be captured or saved in electronic systems.

Document Control

Policy:	Information Security Policy
Date prepared:	October 2020
Dated adopted by SMT:	23/11/2020
Review date:	23/11/2020
Directorate:	Communities and Homes
Department:	Information Technology
Responsible Officer(s):	Corporate ICT Manager Executive Director Deputy Executive Director Senior Management Team Corporate Managers Coordinators, Lead Officers and Supervisors System Administrators All Staff Contractors and Volunteers
Next Review Due:	October 2022
Applicable Legislation A range of legislation, statutes and codes of practice are applicable to information security within the Council. This may include, but is not limited to:	*EU Data Protection Regulation (GDPR) 2016 (applicable from 25 May 2018)* *Human Rights Act 1998* *Freedom of Information Act 2000* *Environmental Information Regulations 2004* *Local Government Acts 1972* *Copyright, Design and Patents Act 1988* *Computer Misuse Act 1990* *Data Protection Act 2018*
Related Policies:	Employee Code of Conduct
Related Procedures:	Information Governance Framework Agile Working Policy Data Protection Policy Sharing Information Safely Policy Clean Desk Policy

Agenda No 7(b)

AGENDA MANAGEMENT SHEET

Report Title:	Licensing Act 2003 – Statement of Licensing Policy 2021-2026
Name of Committee:	Council
Date of Meeting:	15 December 2020
Report Director:	Deputy Executive Director
Portfolio:	Environment and Public Realm
Ward Relevance:	All
Prior Consultation:	A consultation exercise was undertaken as set out within the main body of the report. In addition, members of Licensing and Safety Committee have been consulted on this report prior to publication.
Contact Officer:	John McTernan, Licensing Officer, Tel ext 3539
Public or Private:	Public
Report Subject to Call-In:	No
Report En-Bloc:	No
Forward Plan:	Yes
Corporate Priorities: **(CR) Corporate Resources** **(CH) Communities and Homes** **(EPR) Environment and Public Realm** **(GI) Growth and Investment**	This report relates to the following priority(ies): ☐ To provide excellent, value for money services and sustainable growth ☐ Achieve financial self-sufficiency by 2020 ☐ Enable our residents to live healthy, independent lives ☐ Optimise income and identify new revenue opportunities (CR) ☐ Prioritise use of resources to meet changing customer needs and demands (CR) ☐ Ensure that the council works efficiently and effectively (CR) ☐ Ensure residents have a home that works for them and is affordable (CH) ☐ Deliver digitally-enabled services that residents can access (CH) ☐ Understand our communities and enable people to take an active part in them (CH)

	☐ Enhance our local, open spaces to make them places where people want to be (EPR) ☐ Continue to improve the efficiency of our waste and recycling services (EPR) ☒ Protect the public (EPR) ☐ Promote sustainable growth and economic prosperity (GI) ☐ Promote and grow Rugby's visitor economy with our partners (GI) ☐ Encourage healthy and active lifestyles to improve wellbeing within the borough (GI) ☐ This report does not specifically relate to any Council priorities but
Statutory/Policy Background:	Licensing Act 2003 provides that the Council's Statement of Licensing Policy should be reviewed at least every 5 years.
Summary:	The period of the existing Statement of Licensing Policy expires in January 2021 and, following a period of consultation on a revised Statement of Licensing Policy, this report asks the Committee to recommend Council to adopt a new Statement of Licensing Policy document for the period 2021 to 2026.
Financial Implications:	None
Risk Management Implications:	The Council is required by the Licensing Act 2003 to determine its policy with respect to the exercise of its licensing functions and publish a statement of that policy. Failure to do so could give rise to legal challenges in respect of how it exercises its licensing functions.
Environmental Implications:	None
Legal Implications:	As per the Risk Management Implications.
Equality and Diversity:	Equality Act 2010 considerations are incorporated into the Statement of Licensing Policy. An Equality Impact Assessment is not necessary.
Options:	(a) Recommend the draft Policy without amendment to Council for adoption; (b) Recommend the draft Policy for adoption incorporating any amendments considered necessary after considering the outcome of the consultation exercise

Recommendation:	The Statement of Licensing Policy 2021-2026, as at Appendix 1 to the report, be approved.
Reasons for Recommendation:	The Council is under a statutory duty to review and publish its Statement of Licensing Policy by 7 January 2021.

Agenda No 7(b)

Council - 15 December 2020

Licensing Act 2003 – Statement of Licensing Policy 2021-2026

Public Report of the Deputy Executive Director

Recommendation

The Statement of Licensing Policy 2021-2026, as at Appendix 1 to the report, be approved.

1 Background

1.1 Section 5 of the Licensing Act 2003 requires a licensing authority to prepare and publish a statement of its Licensing Policy at least every five years. During the five year period, the Statement of Licensing Policy must be kept under review and the licensing authority may make any revisions to it as it considers appropriate. If the licensing authority determines and publishes its Statement of Licensing Policy in this way, a new five-year period commences on the date it is published.

1.2 The Council's current Statement of Licensing Policy is valid until 7 January 2021. The draft policy document was prepared in conjunction with the other Warwickshire District Councils and Coventry City Council so that the Council can have, for all intent and purposes, similar policies which assist the trade, the public and responsible authorities.

1.3 The draft Statement of Licensing Policy was fully consulted on and little has changed from the present Statement of Licensing Policy. The draft statement is attached as Appendix 1 to this report.

1.4 Responsibility for adoption of a new Statement of Licensing Policy lies with full Council.

2 The Consultation

2.1 The consultation commenced on 9 October 2020 and ran to 20 November 2020. The draft document was made available on the Council's website and notification of the consultation was sent to the following:

- All responsible authorities
- All Borough Councillors
- All Parish Councils
- Trade organisations
- All licensed premises within the authority area

2.2 No representations have been received in relation to the Statement of Licensing Policy.

Name of Meeting: Licensing and Safety Committee

Date of Meeting: 15 December 2020

Subject Matter: Licensing Act 2003 – Statement of Licensing Policy

Originating Department: Environment and Public Realm

DO ANY BACKGROUND PAPERS APPLY ☐ **YES** ☒ **NO**

LIST OF BACKGROUND PAPERS

Doc No	Title of Document and Hyperlink

The background papers relating to reports on planning applications and which are open to public inspection under Section 100D of the Local Government Act 1972, consist of the planning applications, referred to in the reports, and all written responses to consultations made by the Local Planning Authority, in connection with those applications.

☐ Exempt information is contained in the following documents:

Doc No	Relevant Paragraph of Schedule 12A

Statement of Licensing Policy 2021-2026

Licensing Act 2003

Important Note

In producing this Statement of Licensing Policy the Licensing Authority is aware that the government may amend the Licensing Act 2003, subordinate legislation and statutory guidance.

Any such amendments made in the future will not be incorporated into this policy document and readers of this document are advised to check on the Home Office/Gov.uk website to ensure they have the latest information.

CONTENTS **Page**

STATEMENT OF LICENSING POLICY

1 INTRODUCTION

1.1 Rugby Borough Council ('the Council') has a duty under the terms of the Licensing Act, 2003 ('the Act') to carry out its functions as the Licensing Authority with a view to promoting the following licensing objectives:

- **The prevention of crime and disorder**
- **Public safety**
- **The prevention of public nuisance**
- **The protection of children from harm**

1.2 The promotion of these objectives is the paramount consideration when determining an application and any conditions attached to an authorisation.

1.3 The Borough of Rugby covers an area of 138 square miles located in central England, within the County of Warwickshire. The Borough is on the eastern edge of the West Midlands Region, bordering directly on to the counties of Northamptonshire and Leicestershire, both of which are in the East Midlands Region. The Borough has 41 parishes and the largest centre of population is the attractive market town of Rugby with two thirds of the Borough's 100,100 residents living in the town and the remainder residing in the rural area. The villages in the Borough range in size from 20 to 3,000 people.

1.4 This Statement of Licensing Policy relates to all those licensing activities identified as falling within the provisions of the Act, namely: -

- **The sale by retail of alcohol**
- **The supply of alcohol by clubs**
- **The provision of regulated entertainment**
- **The provision of late night refreshment**

For the purposes of this document any reference to an "authorisation" means a Premises Licence, Club Premises Certificate, Temporary Event Notice (TEN) and where appropriate to the context, a Personal Licence.

1.5 The Council recognises that the licensing function is only one means of promoting delivery of the above objectives and should not therefore be seen as a means for solving all problems within the community. The Council will therefore continue to work with other agencies including neighbouring local authorities, Warwickshire Police ('the police'), the Community Safety Partnership, local businesses, arts organisations, performers, local people and those involved in child protection to promote the common objectives as outlined. In addition, the Council recognises its duty under S.17 of the Crime and Disorder Act, 1998, with regard to the prevention of crime and disorder.

1.6 This policy statement has been prepared in accordance with the provisions of the Act and the Guidance issued under Section 182 of the Act. The Policy statement is valid for a period of 5 years from 7th January 2016. This policy statement will be subject to review and further consultation prior to any substantial changes.

Responsible Authorities

1.7 A list of contact details for responsible authorities authorised under the Act is available on the Council's website.

1.8 The Council has recognised Warwickshire County Council's Multi-Agency Commissioning Team as the local body competent to advise it on the protection of children from harm and has designated it as a responsible authority for the purpose of Section 13 of the Act.

The Licensing Authority as a Responsible Authority

1.9 The Licensing Authority will, when acting as a responsible authority, act in accordance with the Government Guidance issued under Section 182 of the Act wherever possible. In particular, it will not normally intervene in applications where the issues are within the remit of another responsible authority and will ensure an appropriate separation of responsibilities between the officer administering an application and an officer acting as a responsible authority.

Public Health as a Responsible Authority

1:10 There is no specific licensing objective related directly to health within the current legislation. When making representations and available data to other licensing objectives. This may include prevention of accidents, injuries and other immediate harms that can result from alcohol consumption, such as unconsciousness, alcohol poisoning attendance at Accident and Emergency and underage drinking.

1:11 Health bodies hold valuable information which may not be recorded by other agencies, including analysis of data on attendance at emergency departments and the use of ambulance services following alcohol related incidents. Sometimes it may be possible to link ambulance callouts and attendance to irresponsible practices at specific premises and presented to Licensing Sub-Committee when representations are made

2 CONSULTATION

2.1 Before publishing this policy statement the Council has consulted with and given proper consideration to the views of the following in line with the statutory guidance:

- Chief Constable of Warwickshire Police;
- Warwickshire Fire & Rescue Authority;
- Director of Public Health – Warwickshire County Council (Public Health Warwickshire);
- Other responsible authorities;
- Representatives of current licence and certificate holders;
- Representatives of local businesses;
- Representatives of local residents.

3 FUNDAMENTAL RIGHTS

3.1 Under the terms of the Act any person may apply for a variety of authorisations and have each application considered on its individual merits. Equally, any person has a right to make relevant representations on an application or to seek a review of a licence or certificate where provision has been made for them to do so in the Act.

3.2 Applicants and those making relevant representations in respect of applications to the Council have a right of appeal to the Magistrates' Court against the decisions of the Council.

4 LICENSING CONDITIONS

4.1 Licensing is about regulating the carrying on of licensable activities on licensed premises, by qualifying clubs and at temporary events within the terms of the Act. Premises include open spaces. Conditions attached to various authorisations will be focused on matters, which are within the control of individual licensees and others in possession of relevant authorisations. Accordingly, these matters will centre on the premises being used for

licensable activities and the vicinity of those premises. If there is an incident or other dispute, the Council will primarily focus on the direct impact of the activities taking place at licensed premises on members of the public living, working or engaged in normal activities in the area concerned.

4.2 The Council can only impose the national mandatory conditions, unless it has received a relevant representation. This then allows the Council to impose additional conditions, if considered necessary following a hearing.

4.3 When considering any conditions, the Council acknowledges that licensing law should not be seen as the primary mechanism for the general control of nuisance and anti-social behaviour by individuals once they are away from licensed premises and therefore beyond the direct control of the individual, club or business holding the licence, certificate or authorisation concerned. Nonetheless, it is a key aspect of general control and licensing law will always be part of a holistic approach to the management of the evening and night-time economy. For example, applicants should note that stricter conditions to control noise are likely to be imposed in the case of premises situated in largely residential areas.

4.4 The Council does not propose to implement standard licensing conditions on licences or other relevant types of authorisation across the board. Therefore, the Council will attach conditions to relevant authorisations which are tailored to the individual style and characteristics of the premises and events concerned and that are appropriate to promote the licensing objectives in the light of the representations received.

5 OPERATING HOURS

5.1 The Licensing Authority welcomes the opportunities afforded to the local economy by the 2003 Act and will strive to balance this with the rights of local residents and others who might be adversely affected by licensable activities based on the principles laid down in this document.

5.2 When dealing with licensing hours, each application will be dealt with on its individual merits. The Licensing Authority recognises that longer licensing hours with regard to the sale of alcohol can assist to avoid concentrations of customers leaving premises simultaneously. This is expected to reduce the friction at late night fast food outlets, taxi ranks and other sources of transport which can lead to disorder and disturbance. The Licensing Authority does not wish to unduly inhibit the development of thriving and safe evening and night-time local economies which are important for investment and employment locally and in the main welcomed by residents and visitors to the area.

5.3 The Licensing Authority will not set fixed trading hours within designated areas. However, an earlier terminal hour and stricter conditions with regard to noise control than those contained within an application, may be appropriate in residential areas where relevant representations are received and such measures are deemed appropriate to uphold the licensing objectives.

5.4 Shops, stores and supermarkets will generally be free to provide sales of alcohol for consumption off the premises at any times when the retail outlet is open for shopping, unless there are good reasons based on the licensing objectives for restricting those hours.

6 LATE NIGHT LEVY AND EARLY MORNING RESTRICTION ORDER

6.1 The Licensing Authority, having not been presented with evidence to the contrary, does not consider that the application of a Late Night Levy or Early Morning Restriction

Order(s) are appropriate for the Council's area at the present time. The Licensing Authority will keep these matters under review and accordingly reserves the right, should the need arise, to introduce these measures during the life of this statement of licensing policy.

7 CUMULATIVE IMPACT

7.1 For the purposes of this document 'cumulative impact' means the potential impact on the promotion of the licensing objectives of a significant number of licensed premises concentrated in one area. Cumulative impact is a proper matter for the Council to consider in developing its licensing policy. This should not be confused with 'need', which concerns the commercial demand for another particular type of premises. The Government Guidance states that "need" is not a matter for the Licensing Authority but is a matter for the planning authority and the free market.

7.2 The Licensing Authority, having not been presented with sufficient evidence to the contrary, does not consider any area within the Borough to currently have a particular concentration of licensed premises causing a cumulative impact on one or more of the licensing objectives. The Licensing Authority will keep this matter under review and accordingly reserves the right, should the need arise, to introduce a special policy concerning cumulative impact during the life of this statement of licensing policy.

7.3 The absence of a special policy does not prevent any responsible authority or any other party from making representations on a new application for the grant of a licence on the grounds that the premises will give rise to a negative cumulative impact on one or more of the licensing objectives. The Act allows for such consideration but the individual merits of each application must always be considered.

8 PROMOTION OF THE LICENSING OBJECTIVES

Prevention of Crime and Disorder

8.1 Licensed premises, especially those offering late night/early morning entertainment or alcohol and refreshment for large numbers of people, can sometimes be associated with elevated levels of crime and disorder.

8.2 The Licensing Authority expects individual licence/certificate holders, new applicants and temporary event organisers, to regularly review their arrangements in addressing crime and disorder issues pertinent to their particular licensable activities, location and/or premises. Information and advice can be obtained from the Police, business network groups and other sources. The Licensing Authority also encourages local residents and other businesses to discuss issues of concern directly with individual businesses, or, to contact the Police if they believe that particular licensed premises are failing to promote this objective.

8.3 The Council will, through the Community Safety Partnership, devise and help deliver strategies to tackle the misuse of alcohol, which has been identified in the Cabinet Office's Alcohol Harm Reduction Strategy as being a precursor to crime and anti-social behaviour. The Licensing Authority expects existing licence/certificate holders, new applicants and the organisers of temporary events, to be able to demonstrate the measures they use, or propose to adopt, to prevent and actively discourage the sale/supply of alcohol to children and the sale/supply of alcohol to individuals who are already drunk. In general, conditions will reflect local crime prevention strategies.

8.4 The risk assessment approach remains fundamental in the operation of all licensed premises. Licence holders and applicants are strongly recommended to work closely with the Police in particular, in bringing into effect appropriate control measures to either overcome established or potential problems. A combination of short and longer-term

strategies may need to be deployed by authorisation holders to sustain and promote the prevention of crime and disorder.

8.5 The Licensing Authority will expect new applicants, existing licence/certificate holders and organisers of temporary events to adopt recognised good practices in whatever area of operation they are engaged. The Licensing Authority regards the Police as the primary source of advice in relation to preventing crime and disorder and will normally expect Police advice/recommendations to be followed unless there are good reasons for not doing so.

8.6 Queues at late night take-aways can be a source of disorder and applicants for premises licences for this type of premises are expected to address this in their operating schedule.

8.7 The Council has a specific duty under Section 17 of the Crime and Disorder Act 1998 to exercise its functions with regard to the likely effect of doing so on crime and disorder, and also to do all that it reasonably can to prevent crime and disorder in the area. This duty will underpin any control strategy that is employed by the Council who will continue to work in partnership with the Police in addressing crime and disorder issues.

8.8 The Licensing Authority is of the view that generally, in order to promote the licensing objectives; all licensed premises within the Borough are encouraged to be members of the relevant local Pubwatch Scheme, where one exists.

8.9 The Licensing Authority and Police have a zero tolerance of illegal drug use in licensed premises but recognise that drug use is not something that is relevant to all licensed premises. However, it is recognised that special conditions may need to be imposed for certain venues in an effort to prevent the likelihood of drugs being sold and consumed and to create a safer environment for those who may have taken them.

8.10 Once away from licensed premises a minority of consumers may behave badly and unlawfully. There are other mechanisms both within and outside the licensing regime that are available for addressing such issues. The Council will address a number of these issues through the Community Safety Partnership in line with the strategic objectives for crime and disorder reduction and drug and alcohol misuse within the Borough.

8.11 In relation to premises seeking or holding a Premises Licence and where alcohol will be sold under the terms of that licence, the Licensing Authority expects that:

(a) any designated premises supervisor will have been given sufficient management authority and to be able to exercise effective day-to-day control of the premises; and

(b) authority to make alcohol sales when given by the DPS or any other Personal Licence holder should be clearly evidenced in writing.

This is to ensure that premises selling alcohol are properly managed in accordance with the Act and that premises operate in a way that promote the prevention of crime and disorder. This will also benefit operators themselves through being able to demonstrate a commitment to the proper management of premises, particularly if enforcement becomes necessary.

Promotion of Public Safety

8.12 Public safety is not defined within the Act, but the Government Guidance advises that it is concerned with the physical safety of people using the premises and not with public health, which is covered by other legislation.

8.13 Applicants and event organisers will be expected to assess not only the physical environment of the premises (or site) but also operational practices, in order to protect the

safety of members of the public visiting the site, those who are employed in the business, those who are engaged in running an event or anyone else that could be affected by site activities. This assessment would normally take place within a risk assessment framework.

8.14 Holders of premises licences, and club certificates, or those organising temporary events, should interpret 'public safety' widely to include freedom from danger or harm.

8.15 For licensed or certificated premises and for temporary events, public safety must be kept under review and where changes to operational practices/events occur, or the customer profile changes, a review of risk assessments must be undertaken.

8.16 Fire safety is governed by the Regulatory Reform (Fire Safety) Order 2005 and is not something with which the Licensing Authority will normally become involved.

Where a responsible authority has recommended a safe capacity limit on all or part of a premises the Licensing Authority will normally expect an applicant/authorisation holder to follow such a recommendation unless there are good reasons for not doing so.

Prevention of Public Nuisance

8.17 The Licensing Authority remains sensitive to the expectations and needs of different parts of the community in respect of leisure and cultural pursuits, and will view applications accordingly. The impact of those activities on people who have to live, work and sleep within the local vicinity of a licensed premises or event will also be considered. If the impact of licensed activities is disproportionate and unreasonable or markedly reduces the amenity value of the area to local people, then the Licensing Authority will take account of this when exercising its functions.

8.18 The Licensing Authority considers that the potential for public nuisance can be prevented or much reduced by good design and planning during new or ancillary construction works, by the provision of good facilities and effective management. This will require appropriate advice at the planning and development stages of new projects. Applicants should consider carefully the suitability of the premises for the type of activity to be undertaken, particularly in terms of ventilation, noise breakout and noise/vibration transmission to adjoining premises.

8.19 Licence holders already in receipt of complaints should seek an early remedy to any confirmed problem. The organisers of temporary events should pre-empt potential nuisance, especially when complaints have previously arisen at the same venue.

8.20 The Licensing Authority expects authorisation holders to use their risk assessments and Operating Schedules to review and, if need be, to make necessary improvements to the premises, or to operational practices, in order to prevent public or statutory nuisance.

8.21 Where the provisions of existing legislation proves inadequate or inappropriate for control purposes, the Licensing Authority will consider imposing licence conditions. Any condition deemed appropriate and imposed by the Licensing Authority to promote the prevention of public nuisance will focus on measures within the direct control of the licence holder or designated premises supervisor.

Protection of Children from Harm

8.22 The Act details a number of legal requirements designed to protect children in licensed premises. The Licensing Authority is concerned to ensure that authorisation holders including organisers of temporary events, create safe environments (in terms of physical, moral and psychological welfare) for children who may be on the premises. Children

should be unable to access alcohol or drugs and be subject to an appropriate level of care and supervision at all times.

8.23 The Act prohibits children aged under 16 years old and unaccompanied by an adult, from being present in licensed premises (including premises operating under a TEN) that are being used primarily or exclusively for consumption of alcohol

8.24 The admission of children to any premises will otherwise normally be left to the discretion of the individual licensee/event organiser, as the Act does not generally prohibit children from accessing licensed premises. Where children are accompanied and supervised by a responsible adult, additional measures should not normally be necessary. The Licensing Authority supports the view that children should enjoy access to a range of licensed premises where possible, but cannot impose conditions requiring the admission of children to any premises.

The Licensing Authority will judge the merits of each separate application before deciding whether or not to impose conditions restricting access by children. Conditions which may be relevant in this respect are outlined in the Government Guidance.

8.25 In premises where alcohol is sold or supplied it is a mandatory condition that premises licence holders will operate a recognised "Proof of Age" scheme. The Council supports the Challenge 25 scheme and where this is not proposed within the operating schedule, alternative and similarly rigorous controls should be detailed.

8.26 The Licensing Authority expects that customers should be confronted by clear and visible signs on the premises that underage drinking constitutes an offence in law and that they may well be required to produce proof of their age to a member of staff. Organisers of temporary events should apply similar safeguards in their undertakings.

8.27 Venue operators seeking premises licences and club premises certificates can volunteer prohibitions and restrictions in their operating schedules because their own risk assessments have determined that the presence of children is undesirable or inappropriate. These will become conditions attached to the licence or certificate where no relevant representations are received by the Licensing Authority.

8.28 The Licensing Authority regards Warwickshire County Council's Multi Agency Commissioning Team as being the primary source of advice and information on children's welfare and would normally expect any advice/recommendations from them to be followed unless there are good reasons for not doing so. The Licensing Authority will attach appropriate conditions where these appear appropriate to protect children from moral, psychological or physical harm, or sexual (or, indeed, any form of) exploitation.

8.29 In order to prevent children from seeing films incompatible with their age, licence holders who exhibit films will be expected to impose and enforce viewing restrictions in accordance with the recommendations of the British Board of Film Classification.

8.30 It is expected that authorisation holders will ensure that, whenever children are in the vicinity of a film or exhibition that is being shown/staged in a multi purpose premises, sufficient ushers/stewards (minimum 18 years old) will be in attendance at the entrance to the viewing rooms at all times to ensure children cannot enter or view the film or exhibition.

8.31 Children have access to a range of regulated public entertainment venues and may be present as members of a viewing audience or as performers in their own right. The Licensing Authority expects authorisation holders including those organising temporary public events, to make proper provision for child safety and welfare during such events. Notwithstanding public safety issues, supervisory arrangements must be reflected within operating schedules. Suitable monitoring strategies should also be in place to ensure that supervisory levels are appropriate.

8.32 Where a large number of children are likely to be present on any licensed premises, for example, a children's show or pantomime, the Council may require that there is an adequate number of adult staff at places of entertainment to control access and egress of children and to protect them from harm. Children present at events as entertainers will be expected to have a nominated adult responsible for each child performer.

9 MANDATORY LICENSING CONDITIONS

9.1 The Government has introduced a range of mandatory conditions aimed at establishing minimum standards for the way alcohol is sold. The conditions apply in some form to all alcohol retailers.

10 OTHER CONSIDERATIONS

Relationship with Planning

10.1 The planning and licensing regimes involve consideration of different (albeit related) matters. The Licensing and Safety Committee and Sub-committees are not bound by decisions made by the Council's Planning Committee, and vice versa.

10.2 The grant of any application or variation of a licence which involves a material alteration to a building would not relieve the applicant of the need to apply for planning permission or building control approval, where appropriate.

10.3 There are also circumstances when as a condition of planning permission, a terminal hour has been set for the use of premises for commercial purposes. Where these hours are different to the licensing hours, the applicant must observe the earlier closing time. Premises operating in breach of their planning consent would be liable to enforcement action under planning law.

10.4 The Local Planning Authority may also make representations against a licensing application in its capacity as a responsible authority, where such representations relate to one or more of the licensing objectives (see Paragraph 1.1 above).

Applications

10.5 An applicant may apply under the terms of the Act for a variety of authorisations and any such application will be considered on its individual merits. Any person may make representations on an application or seek a review of a licence or certificate where provision has been made for them to do so in the Act.
Representations should be made directly to the Licensing Authority by writing to Rugby Borough Council, FAO Public Health and Licensing Team, Town Hall, Evreux Way, Rugby CV21 2RR or licensing@rugby.gov.uk

10.6 The Licensing Authority expects each and every applicant for a premises licence, club premises certificate or variation to demonstrate how they intend to meet the licensing objectives. Where no information is given by the applicant, there may be circumstances where the Licensing Authority considers the application to be incomplete and the application is returned without further processing.

10.7 In determining a licence application the Licensing Authority will take each application on its merits. Licence conditions, other than those volunteered by the applicant in the Operating Schedule or by agreement with a responsible authority, will only be imposed in order to promote the licensing objectives following a hearing and will only relate to matters within the control and ability of the applicant. Licence conditions will not normally be imposed where other regulatory provision is in force (e.g. planning, environmental health, fire safety, and building control legislation) so as to avoid confusion and duplication, except where they can be exceptionally justified to promote the licensing objectives.

10.8 The Licensing Authority will impose only such conditions as are proportionate towards promoting the licensing objectives and which do not propose unnecessary burdens and which are appropriate to the individual size, style and characteristics of the premises and events concerned.

10.9 In considering applications, the Licensing Authority will primarily focus on the direct impact of the activities taking place at the licensed premises on members of public living, working or engaged in normal activity in the area concerned. The Licensing Authority recognises that licensing law is not the primary mechanism for the general control of nuisance and anti-social behaviour by individuals once they are away from the licensed

premises and, therefore, beyond the direct control of the individual, club or business holding the licence, certificate or authorisation concerned.

10.10 Conditions include any limitations or restrictions attached to a licence, certificate or other authorisation and essentially are the steps or actions the holder of the authorisation will be required to take or refrain from taking at all times when licensable activities are taking place at the premises in question.

Live Music Act

10.11 The Live Music Act came into force on 1st October 2012 and is designed to encourage more performances of 'live' music. The Act removed live music from the scope of Licensing Authority control, subject to certain criteria. However, controls may be added or reinstated at a review hearing if the manner in which live music has been provided has been undermining the licensing objectives.

11 BEST PRACTICE SCHEMES

11.1 The Council supports best practice schemes for licensed premises. If your premises are in an area covered by a scheme, you are encouraged to become a member of the scheme. Schemes, set up by local businesses, have adopted an agreed approach to reduce crime and disorder in the area by excluding those whose presence on their premises pose a risk to a safe drinking environment.

12 INTEGRATING STRATEGIES AND THE AVOIDANCE OF DUPLICATION

12.1 By consulting widely prior to this policy statement being published, the Council has taken full account of local policies covering crime prevention, anti-social behaviour, culture, transport, planning and tourism. Many of these strategies may not be directly related to the promotion of the licensing objectives, but indirectly impact upon them.

12.2 There are a number of wider issues which may need to be given due consideration when dealing with applications. The Council's Licensing and Safety Committee can request reports, where it thinks it is appropriate on the following areas:-

- the needs of the local tourist economy to ensure that these are reflected in their considerations;
- the employment situation and the need for new investment and employment where appropriate; and
- the general impact of alcohol related crime and disorder, by providing regular reports to the planning committee. This will enable the planning committee to have regard to such matters when taking its decisions and avoid any unnecessary overlap.

Duplication

12.3 When considering any application, the Council will avoid duplication with other regulatory regimes so far as possible. Therefore, the Council will not attach conditions to a licence in relation to a matter covered by another regulatory regime unless going beyond such a regime is considered appropriate for the promotion of the licensing objectives in the particular circumstances.

Promotion of Equality

12.4 The Licensing Authority in carrying out its functions under the Act is obliged to have 'due regard' to the need to eliminate unlawful discrimination harassment and victimisation, to advance equality of opportunity and to foster good relations between persons with different protected characteristics. The protected characteristics are age, disability,

gender reassignment, pregnancy and maternity, race, religion or belief, sex and sexual orientation.

The Government Guidance advises that conditions should not be attached to authorisations which would duplicate existing statutory requirements. The Council therefore takes this opportunity to remind operators of premises of their duties towards disabled persons (including performers) on their premises under the Building Regulations and the Equalities Act 2010. This includes a duty that any person who provides a service to the public must make reasonable adjustments to any physical feature that makes it impossible or unreasonably difficult for a disabled person to access a service, or to provide the services by a reasonable alternative means.

13 ENFORCEMENT

13.1 The Licensing Authority has an established working relationship with the Police and other enforcing authorities on enforcement issues. This will provide a more efficient deployment of resources targeting high risk premises and activities.

13.2 The Council's enforcement regime in relation to licensing follows the Government's Regulators' Code in that it follows the basic principles of Openness, Helpfulness, Proportionality and Consistency.

13.3 Licensed premises may be visited by the responsible authorities and the Licensing Authority to carry out targeted inspections to check that the premises licence/certificate is being complied with, to check compliance with other legislation and/or to deal with a complaint that has been received.

13.4 On occasions a multi-agency group (representing a number of responsible authorities) may visit the premises. Officers will inspect the areas of the premises relevant to their particular role.

13.5 There are several enforcement options available depending on the outcome of an inspection or complaint which include:

- Verbal advice – this covers minor complaints/infringements where advice is seen as the most appropriate way to deal with the issue.
- Written warning – this is a step-up from verbal advice and authorisation holders are given a letter recording the warning given and containing the details of any necessary remedial action.
- Action planning – this plan will be written down and given to the authorisation holder. It explains what actions are required in order to comply with the licensing objectives, specific legislation or conditions and within what time period. The action plan will be regularly reviewed will be terminated if complied with. If there are areas of non-compliance, the authorisation holder may face prosecution or the authorisation may be called for a review.
- Review – when there is evidence to show that the licensing objectives are not being met then a review application may be made and this will be heard by a Licensing Sub-Committee. A decision will be made by the Sub-Committee based on the evidence put forward as to what action, if any, should be taken. This can be removal of the DPS and/or revocation, suspension or amendment of the authorisation or the imposition of additional conditions.
- Prosecution – under the Licensing Act, certain offences can be instituted by the Licensing Authority / Director of Public Prosecutions / the Weights and Measures Authority (Trading Standards). In addition, responsible authorities have a wide range of powers to institute prosecution under other specific legislation depending on the nature of evidence found.
- Closure – several of the responsible authorities have the power to close licensed premises whilst on site if they deem it necessary e.g. the Police, Health & Safety,

Environmental Health, Trading Standards and the Fire Service. The Licensing Team also have powers to request closure through the Magistrates' Court for continuing unauthorised alcohol sales.

14 ADMINISTRATION, EXERCISE AND DELEGATION OF FUNCTIONS

Licensing and Safety Committee

14.1 The powers of the Council under the Act may be carried out by the Licensing and Safety Committee, by a Sub-Committee or by one or more Council officers acting under delegated authority.

14.2 It is considered that many of the decisions and functions will be purely administrative in nature. In the interests of speed, efficiency and cost effectiveness, the Licensing and Safety Committee may delegate these functions to Sub-Committees, or in appropriate cases, to officers supporting the licensing function.

14.3 Where under the provisions of the Act there are no relevant representations on an application these matters will be dealt with by officers. Should there be relevant representations then an oral hearing will usually take place before a Licensing Sub-Committee, except where all parties agree to proceed in writing. A licence/certificate review will normally take place before a Licensing Sub-Committee. The Council's scheme of delegation can be found in its Constitution which is available at www.rugby.gov.uk.

Matters to be dealt with	Full Committee	Sub Committee	Officers
Application for a personal licence		If a police/home office objection	If no objection made
Application for a premises licence/club licence premises certificate		If a relevant representation made	If no relevant representation made
Application for provisional statement		If a relevant representation made	If no relevant representation made
Application to vary designated premises supervisor		If a relevant representation made	If no relevant representation made
Application to transfer of premises licence		If a police objection	All other cases
Application for interim authorities			All cases
Application to review premises licence/club premises certificate		If a police objection	All other cases
Application for interim authorities		If a police objection	All other cases
Application to review premises licence/club premises certificate		All cases	
Decision on whether a complaint is irrelevant, frivolous or/and vexatious etc.			All cases
Decisions to object when local authority is a consultee and not the relevant authority considering the application	All cases		
Determination of a police/EHO objection to a temporary event notice		All cases	
Determination of a Minor Variation application			All cases
Removal of the requirement for a designated premises supervisor at community premises		If a police objection	All other cases

Application forms and process

14.4 The application form will be in the prescribed format. The operating schedule will form part of the completed application form for a premises licence and a club premises certificate. The form will need to contain information that describes the style of the venue, the licensable activities to be provided, the operational procedures, hours, nature of the location, needs of the local community, etc. Most importantly, the applicant will have to detail the steps that will be taken to promote the licensing objectives. Applicants should carry out a risk assessment before they apply for a licence.

14.5 Applicants are encouraged to fully consult the Police and other statutory services well in advance of carrying out their risk assessments and submitting their applications. Application forms and guidance leaflets will be available from the Licensing Team, including contact names for each of the responsible authorities that will be receiving copies of applications. Most applications will require additional documentation and a fee to be included with the form. Incomplete applications will not be considered and will be returned to the applicant.

14.6 Where national guidance permits, on line applications will be accepted providing the necessary documentary attachments are uploaded into the application and the appropriate fee paid. Rugby uses the Electronic Licence Management System (GOV.UK) which is supported by the Department of Business Innovation and Skills.

14.6 Applicants are encouraged to make themselves aware of any relevant planning and transportation policies, tourism and cultural strategies and local crime, alcohol, drug and disorder strategies in order to take these into account, where appropriate, when formulating their operating schedule.

14.7

Changes to the Licensing Act 2003, under The Immigration Act 2016

• An “Entitlement to Work” test introduced for Personal Licence Holders and individual Premises Licence Holders, where the Premises Licence permits the sale of alcohol or late night refreshment;
• Applicants for Personal Licences must produce evidence of their entitlement to work in the United Kingdom;
• Where the applicant has committed immigration offences, the Licensing Authority to advise the Secretary of State (Home Office Immigration Enforcement (“HOIE”)) as it would the Police on conviction of a “Relevant Offence”;
• Applicants for Premises Licences, made by individuals, will likewise have to produce evidence of their entitlement to work in the United Kingdom, along with their nationality and date of birth;
• Individual applicants for a transfer of a Premises Licence must provide evidence of their entitlement to work in the United Kingdom, along with their nationality and date of birth;
• Applicants to become a Designated Premises Supervisor must provide their place of birth, date of birth and nationality and confirm on their consent to become the Designated Premises Supervisor that they are entitled to work in the United Kingdom;
• The Secretary of State (HOIE) is a Responsible Authority;
• Applications for the transfer of a Premises Licence also need to be served on the Secretary of State (HOIE), as well as the Police and Licensing Authority;
• If an individual holding a Premises Licence ceases to be entitled to work in the United Kingdom on or after 6th April 2017, the Premises Licence lapses immediately, and will lapse completely unless transferred or an Interim Authority lodged within 28 days;
• A Personal Licence will lapse when an individual is no longer entitled to work in the United Kingdom on or after 6th April 2017;
• Applications for transfers or new Premises Licences must not be signed by PA, since they contain a declaration of the individual’s entitlement to work in the United Kingdom;

• Immigration Officers can now enter licensed premises as if they were a Police Constable, if premises are being used for the sale of alcohol or late night refreshment, to see if an offence under The Immigration Act 2016 has been committed.

These changes in processing, checking and determining applications has already come into force but were introduced after the final draft of the previous policy.

Who do the changes apply to?

The amendments apply not only to licences permitting the sale of alcohol but also to those relating to late night refreshment.

The Secretary of State is entitled to object to an application when they consider that the exceptional circumstances of the case are such that granting the application would be prejudicial to the prevention of illegal working in licensed premises.

The Licensing Authority has responsibility to serve online applications on all Responsible Authorities and they too will now need to include the Secretary of State.

The address for postal applications is The Home Office, Alcohol Licensing Team, Lunar House, 40 Wellesley Road, Croydon CR9 2BY.

What effect will the changes have?

The amendments to the Licensing Act establish that individuals resident in the UK will not be able to apply for a premises licence unless they are entitled to work here. Also, a premises licence will lapse if the holder ceases to be entitled to work.

Individuals resident in the UK who are not entitled to work will not be permitted to apply for a transfer, either. Transfers can be objected to within 14 days by the Secretary of State on the above mentioned ground.

Those not entitled to work in the UK will not be permitted to apply for a personal licence and if a personal licence holder’s employment status changes and they are no longer allowed to lawfully work, then their licence lapses. This has an obvious implication if they are the Designated Premises Supervisor.

The amendments also make a number of offences under the Immigration Act relevant for the purposes of applying for personal licences.

Illegal Working Closure Orders can be issued by Immigration Officers if they are concerned that breaches of the requirements are being made.

This will prevent access to the premises and prohibit paid or voluntary work taking place therein. Such Orders can last for up to

15 COMMENTS ON THIS POLICY

15.1 The Statement of Licensing Policy will be reviewed on a regular basis. Individuals and organisations wishing to comment on the policy are invited to send their comments in writing to:

Public Health and Licensing Team
Environmental Services
Town Hall
Evreux Way
Rugby CV21 2RR

Telephone Number: 01788 533533
e-mail: licensing@rugby.gov.uk
website www.rugby.gov.uk

If you need this information in another format please contact the Licensing Team:

Telephone: 01788 533533
E-mail: licensing@rugby.gov.uk