www.rbwm.gov.uk

Royal Borough
of Windsor &
Maidenhead

Royal Borough Windsor & Maidenhead

Supplier and Third-Party IT Acceptable Usage Policy

June 2020

“Building a borough for everyone – where residents and businesses grow, with opportunities for all”

Our vision is underpinned by six priorities:

Healthy, skilled and independent residents
Growing economy, affordable housing
Safe and vibrant communities
Attractive and well-connected borough
An excellent customer experience
Well-managed resources delivering value for money

CONTENTS

Frequently used acronyms

IT	Information Technology
RBWM	Royal Borough of Windsor & Maidenhead

1 PURPOSE

1.1 This policy defines the security conditions for external suppliers, contractual third parties and agents, external organisations and others who provide services to the council using IT facilities.

1.2 The IT facilities they use may either be council IT facilities or their own. All the above are required to read the policy and confirm agreement in writing by completing the Secure Portal Access Agreement Form.

2 SCOPE

2.1 This RBWM Supplier and Third-Party IT Acceptable Usage Policy ensures the Royal Borough of Windsor and Maidenhead implement the correct processes and procedures relating to the acceptable access and usage of the RBWM Portal and IT facilities.

2.2 This RBWM Supplier and Third-Party IT Acceptable Usage Policy aims to ensure that the integrity and security of the council's data and other resources remain protected.

2.3 The "Portal" is defined as either a secure website that offers a variety of online services, or remote access Virtual Private Network (VPN) connections such as Site 2 Site (Fixed) or dial on demand VPN Connections (Flexible).

2.4 The council recognises the risks associated the use of IT facilities and when handling council information when conducting council business.

2.5 The policy aims to reduce risks arising from:

2.5.1. unauthorised access to buildings, IT equipment or systems.

2.5.2. loss, theft, or misuse of information.

2.5.3. misuse of IT systems.

2.5.4. legal non-compliance.

2.6 Additional security requirements contained in the supplier's or external organisation's own Information Security policies and procedures are not covered by this policy.

3 APPLICABILITY

3.1 This In this policy the "Supplier", "Partner" or "Third-Party" is an organisation and its employees who apply to access the Council's IT facilities and information through the RBWM Internet Portal. This access can be for a variety of reasons including IT support, collaborative working between RBWM and other organisations, or for commissioned work for the Council.

3.2 All partners, suppliers and third parties requiring access to the Council's IT facilities using the RBWM Internet Portal must read this document before completing and signing the **Secure Portal Access Agreement Form**.

3.3 The Secure Portal Access Agreement Form must be returned with the signature of everyone who will use the Portal and the supporting signature of:

3.3.1. The RBWM manager responsible for the access request, and.

3.3.2. The signature of either:

- a senior company representative, e.g. Director; for commercial companies; or

- a senior manager for not-for-profit or public sector organisations.

4 AUTHORISATION

4.1 Only authorised persons should have access to council assets and systems or accessing the council IT or mobile network. Any user that deliberately or inadvertently accesses the council IT or mobile network or systems unauthorised, will be in breach of this policy.

4.2 For any council business:

4.2.1. Users accessing council IT facilities must comply with all council policies and procedures.

4.2.2. Managers and Team Leaders must ensure their staff comply with this policy and provide advice to them.

4.2.3. Managers and Team Leaders must ensure security incidents are raised in response to IT access security concerns or security breaches as covered in the **Reporting Security Incidents Policy**.

4.2.4. IT Services provide technical solutions to support different IT access security levels, depending on the sensitivity and value of the data accessed. Administer, control and monitor access to IT facilities and systems.

4.2.5. IT Services ensure that privileged and systems administrator access is strictly controlled based upon a valid business justification and specific job requirements as approved by the user's line managers.

5 POLICY COMPLIANCE

5.1 **Compliance Measurement**

5.1.1. All users must comply with this policy.

5.1.2. The IT Support will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.1.3. If you do not understand the implications of this policy, how it may apply to you, or your security responsibilities when working with the council, please seek advice in advance from your line-manager or contact the council's Data Protection Officer at **dpo@rbwm.gov.uk**.

5.2 **Exceptions**

5.2.1. Any exception to the policy must be approved by the IT Senior Management Team in advance.

5.3 **Non-Compliance**

5.3.1. Any breach of this policy may be subject to disciplinary action under the council's disciplinary procedures, up to and including dismissal. In circumstances where it is believed that a criminal offence has been committed the matter may be reported to the Police.

6 ACCESS CONTROL

6.1 Never attempt to access council IT facilities without written permission, and only use authorised equipment at authorised locations.

6.2 Only access the council's IT facilities by using the user identifier and password provided by the council. Also ensure that passwords used are difficult to crack and changed regularly.

6.3 Protect and never disclose council-issued user identifiers and passwords, and only use the user identifier(s) in an agreed manner.

6.4 Only access the council’s IT facilities remotely by using a secure technology configuration and security framework as provided or defined by the council.

6.5 Never exchange data on portable media with the council, e.g. on USB memory sticks or DVD/CDs, without council authorisation. These media must be kept secure and locked away when not in use.

6.6 Always use the council’s data exchange policies and procedures to provide security for once-off transfers of personal or sensitive data to or from the council.

7 INFORMATION AND DATA HANDLING SECURITY

7.1 Always seek to prevent accidental disclosure of the council’s sensitive or personal information, e.g. by the accidental overlooking or overhearing of such information.

7.2 To handle personal or sensitive council data, emails, or information with care, for example:

7.2.1. Use courier despatch for highly sensitive or personal data. It is recommended that this type of information be hand delivered or delivered by a personal courier.

7.2.2. Do not leave printout containing personal or sensitive information unattended when printing

7.2.3. Hold telephone conversations in private areas, so that they cannot be overheard.

7.2.4. Keep personal or sensitive information or data locked away when not attended.

7.2.5. Dispose of this information by using a cross-cut shredder or a confidential waste service.

7.3 Protect and handle securely any electronic or paper council information when it is used, sent, received, stored, or processed.

7.4 Never disclose any sensitive or personal council information unless satisfied that the recipient(s) have a ‘need to know’ and are authorised by the council to see it.

7.5 Never send files, web service data, or emails that contain sensitive or personal data across the public Internet without providing encryption protection.

8 SECURITY RESPONSIBILITIES

8.1 Ensure that any personnel security checks required by the council for individuals providing services to the council are completed and the results are checked and accepted before accessing the council's IT facilities or information.

8.2 The council manager responsible for the service(s) provided must define the security checks required. This will ensure appropriate protection of the council's interests.

8.3 Take responsibility for secure use of council IT services and secure access to council information. This includes protecting and never disclosing user identifiers, passwords, access tokens, or any other access mechanisms

9 PHYSICAL AND ENVIRONMENTAL SECURITY

9.1 Return, or securely destroy in an agreed fashion, any council information or data used in the provision of services.

9.2 Take precautions to protect all computer media, portable computers, and electronic equipment (e.g. Internet phones) when carrying them in transit. For example, never leave a laptop, other equipment, or computer media, unattended.

10 SECURITY INCIDENT REPORTING

10.1 Report all suspected or actual IT security concerns or security breaches to the council manager responsible, who can complete a Security Incident Report.

10.2 Also inform the council's IT Services as soon as possible to ensure that electronic equipment can be disabled if possible.

11 PROTECTION AGAINST DAMAGE AND CYBER ATTACKS

11.1 Never knowingly cause any form of damage to the council's IT facilities, nor attempt to bypass or subvert system security controls.

11.2 Never insert portable computer media into the council's IT network or devices.

11.3 Ensure that any IT equipment used to provide services to the council is protected by antivirus software and spyware, and that this software and any anti-virus definitions are always up to date. Also never knowingly introduce viruses or other malware into the council’s IT network; nor knowingly disable anti-virus protection.

11.4 Where a virus is suspected or detected, the matter must be reported to the council’s IT Services immediately. An infected computer must not be used until the virus was removed by authorised IT support staff and the device was scanned and cleared.

11.5 Never download software or programs (including screen savers and wallpaper) from the Internet or from removable media onto council IT equipment.

11.6 Software must only be installed onto council IT equipment by authorised staff.

11.7 Never disable any IT security safeguards that have been implemented on computer equipment used to provide the council with services.

12 TERMINATION OF WORK

12.1 Before termination of the contract or work agreement, inform the council of any information held, and ensure that this information is either destroyed, stored under an agreement, or formally returned to the council.

12.2 Notify the council immediately if a provider of services to the council terminates their employment, or changes job, and their access to council IT facilities is no longer required.

13 CONTROL OF CHANGES

13.1 Ensure that all changes made to the council’s IT programs, databases or files are authorised and documented and approved within the council’s IT Change Control process.

APPENDICES

RELATED STANDARDS, POLICIES AND PROCEDURES

- Reporting Security Incidents policy.
- Secure Portal Access Agreement Form.
- The Computer Misuse Act 1990.
- UK Data Protection Act 2018
- Information Security Management Standard ISO/IEC 27001:2013
- NIST SP800-63.3 standards.

Document Name	**Supplier and Third-Party IT Acceptable Usage Policy**		
Document Author	**Security manager**		
Document owner	**Head of HR, Corporate Projects and IT**		
Accessibility			
File location			
Destruction date			
How this document was created	Version 1	**18/07/2011**	**Security manager**
	Version 2	**19/09/2017**	**Security manager**
	Version 3	**25/06/2020**	**Infrastructure security manager**
Circulation restrictions			
Review date	**25/06/2022**		