www.rbwm.gov.uk

Royal Borough of Windsor & Maidenhead

Royal Borough Windsor & Maidenhead

Information Technology Access Security 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 The purpose of this IT access security policy is to ensure that the applicable and relevant security controls are set in place in line with the Royal Borough of Windsor and Maidenhead and Her Majesty's Government (HMG) requirements.

1.2 Unauthorised access to the council's data and IT facilities can result in a serious threat to individuals or to the council. To counter this threat IT access security controls are needed to reduce the risk of unauthorised access to systems and data. Benefits arising include fewer security breaches and lower support costs.

1.3 This policy recognises the increased risk to personal information, and it compliments, but do not replace the council's procedures and guidelines regarding protecting council information which are covered separately in the **Information Handling Policy** which can be found on the council's web site and should be read in conjunction with this policy.

2 SCOPE

2.1 The IT access security policy ensures the Royal Borough of Windsor and Maidenhead implement the correct processes and procedures relating to IT access. This policy is aimed at all users who are authorised to use computing equipment ensuring they are aware of the security risks relating to IT access and comply with the council's confidentiality and security standards.

2.2 Specific IT access security rules and procedures must be defined by the council to ensure its IT facilities, systems and data are protected against unauthorised access.

2.3 All persons authorised to access council IT facilities, systems or data must comply with these rules and procedures. The policy applies to any person accessing council IT facilities or electronic data in any format, on any device, and from any location.

2.4 Physical access security is not included and is covered separately in the **Security Code of Conduct Policy** which can be found on the council's web site.

2.5 This policy covers the use of electronic information assets such as computer devices – computers, laptops, notebooks, tablet computers, PDA's and work-issued mobile phones (smartphone's eg, iPhones, windows phones etc); purchased or authorised by RBWM and apply to all RBWM staff, including temporary, contractors and third-party members.

3 APPLICABILITY

3.1 This policy applies to all council employees and RBWM Councillors. This policy also applies to contractors, temporary, agency staff, partners and others working in a similar capacity that can access, manage, or process information assets of the council. They are also accountable for understanding and adhering to the guidance contained in this policy and any applicable supporting policies and procedures. All applicable persons listed above are referred to as 'users' in this policy.

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:

- Users accessing council IT facilities must comply with all council policies and procedures.
- Managers and team leaders must ensure their staff comply with this policy and provide advice to them.
- 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**.
- IT services provide technical solutions to support different IT access security levels, depending on the sensitivity and value of the data accessed.
- IT services ensure that privileged and systems administrator access is strictly controlled for the applications they administer 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. IT Services 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 RESPONSIBILITIES AND RISK

6.1 All users have a responsibility for the safety and security of council equipment. This applies to working in the office/work environment as well as working out of the office.

6.2 Everyone needs to be security conscious and follow common-sense rules with further guidance on asset management as covered in the **Electronic Information Asset Management Policy** which can be found on the council's web site and should be read in conjunction with this policy.

6.3 It is a user's responsibility to prevent their username / user identifier and password being used to gain unauthorised access to council systems by following the security rules outlined in this policy.

6.4 Any changes to staff roles and access requirements must be communicated by the line manager or team leader to IT services or an authorised systems administrator.

7 SECURITY MEASURES

7.1 To reduce the risk of unauthorised access the council has put the following measures in place:

- Encryption is applied to all computing equipment.
- Password protected screensavers are installed on laptops.
- Anti-virus software is in use and is updated with the latest antivirus signatures.
- Secure disposal of computing equipment is recorded in the asset register.
- No data should be stored on mobile equipment.

- Always wear your identity badge visibly when you are on council business or in council buildings.

- Escort anyone in council buildings without an identity badge to reception.

- Escort visitors around the building whenever possible.

8 USER IDENTIFIERS AND PASSWORD MANAGEMENT

8.1 Passwords are the first line of defence for IT systems and, together with personal user identifiers and IT access codes, establish that users are who they claim to be. A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of the council's computers and systems and can compromise the council's entire infrastructure.

8.2 Username / user identifiers and passwords / passphrases are covered in detail in the **Password Policy** which can be found on the council's web site with further guidance on passwords and should be read in conjunction with this policy.

9 ACCESS PROCEDURES

9.1 Use of council computing resources requires registration and granting of access rights by:

- IT services,

- an approved IT support service, or

- by a nominated systems administration role within a council service.

9.2 When using the council's IT facilities, it is every user's responsibility to comply with any security conditions and the council's information security policies. Users must have previously confirmed their responsibilities in a signed employment contract, a confidentiality clause, or a security declaration.

9.3 Systems access authorisation may be withheld, withdrawn, or suspended at any time by the IT service, or by the responsible council service. This may be in the interests of security; for maintenance purposes; or to prevent possible abuse or misuse.

9.4 Granting of IT access rights will normally be by the provision of a username / user identifier and password. Higher level security facilities may require any of these additional safeguards: additional PIN numbers, two factor authentication, physical security tokens, or personnel security checks.

9.5 Any query or complaint about access, or about authorisation to use IT systems should be referred to IT services in the first instance.

9.6 All council IT facilities must be configured to enforce the following:

- Protection with regards to the retrieval of passwords and security details.
- System access monitoring and logging at a user level.
- Password administration procedures must be secure, documented, and auditable.

10 UNAUTHORISED ACCESS

10.1 Precautions must be taken to reduce the risk of unauthorised IT access to any council network, system, physical media, and devices used for processing.

10.2 Users must restrict access to any publicly accessible network jacks.

10.3 Users must always lock computing devices (e.g. by logging out or by using control-alt-delete-space/enter) before leaving it unattended to prevent unauthorised access.

10.4 Users must use password-protected screen savers with time delays to prevent unauthorised access when users forget to lock computing devices before leaving it unattended.

10.5 Users must shut down and switch off computing devices at the end of the working day.

11 USER ACCESS

11.1 User access control procedures must be documented, implemented, and kept up to date to prevent unauthorised access.

11.2 A request for access to council facilities or IT application systems must be submitted for approval by using the appropriate **Request / Amend Access Form** for all council employed staff, Achieving for Children staff, Optalis staff and Partner Organisations. A line-manager or team leader must approve the request.

11.3 Users, or their line managers, must notify IT services of any change in status which may affect their right to use council IT facilities.

11.4 The **Request / Amend Access** process extends from the initial registration of **New Employee** to the final de-registration of **Leavers** who no longer require access.

11.5 Each user must be allocated access rights and permissions that are appropriate for the tasks they perform. They will have a unique login and password that is used every time they log on to a system.

11.6 User IT access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated.

11.7 System administration accounts must only be provided to users who are required to perform IT administration tasks in their job role.

11.8 System administration accounts must be disabled immediately when no longer needed.

12 SHARED USER ACCESS

12.1 Sharing a user identifier for access with others is a security risk. It is much less secure than having an individual identifier because there is no audit trail showing who is logged on at any one time. A strong business justification is required.

12.2 Only in exceptional situations a shared (generic) user account may be authorised by the IT service, on receipt of the appropriate authorisation request.

12.3 If a shared user account is approved, the authorising manager will be responsible for the following additional security measures:

- Maintenance of an up to date list of all users authorised to use the shared account.
- Training for all users of the shared account to ensure they understand the security risks and how to minimise them.
- Maintaining an audit trail showing who is using any shared identifiers at any time.

12.4 Security measures may be audited.

13 APPLICATION ACCESS

13.1 Access to data accessed through applications must be restricted using security features like groups, policies, and appropriate access rights.

13.2 The business owner of the software application is responsible for ensuring appropriate and secure access to the system.

13.3 The business owner of the software application is responsible for ensuring access to the system has been removed for any user that doesn't require it anymore (when a user left the council, user was suspended, user on long term leave or illness, etc).

14 NETWORK ACCESS

14.1 The connection of unchecked or privately-owned computers (or portable electronic devices) to the council's network can seriously compromise network security if they are infected by malware or viruses.

14.2 Connecting any privately-owned equipment from individuals or other organisations to the council's network is not allowed. Explicit approval must be obtained from IT services.

14.3 Where remote access to the council IT network is required, a request must be made to IT services for access authorisation and set-up.

14.4 For organisations or individuals working outside the council an external portal set-up request must be submitted before external access to the council's IT network is permitted. Partners or third-party suppliers must contact IT services before first connecting to the council IT network. Access will be logged and may be monitored.

15 REMOTE ACCESS

15.1 Remote access must be secured and strictly controlled with encryption by using firewalls and secure 2-factor-authentification Virtual Private Networks (VPNs).

15.2 Hosts that are connected to the council network must be fully patched and updated with the most up-to-date anti-virus signature.

15.3 The user should be completely responsible to ensure not to violate any of the council's policies, and that they don't perform any illegal activities, and don't use the access for outside business interests while accessing the council network remotely.

15.4 Remote access is covered in a separate policy **Remote Working Security Policy** with further guidance on remote working and should be read in conjunction with this policy.

16 PRIVILEGED ACCESS

16.1 System administrators and IT support staff may require additional privileged access (elevated or administrator access) accounts. This access must be via a unique login identifier that can be traced back to an individual. The privileged login identifier must not give any indication of the level of access that it provides to the system.

16.2 IT services must ensure that privileged account access for the applications they administer is strictly controlled and based upon valid business justification and specific job requirements.

16.3 IT services must monitor access to privileged accounts.

16.4 Privileged access to council computing resources shall only be used for official council business. While the council permits reasonable personal use of computing resources, this is restricted to non-administrative activities.

16.5 Use of elevated or administrator Access should be consistent with an individual's role or job responsibilities as prescribed by their manager. When an individual's role or job responsibilities change, privileged access should be appropriately updated or removed. In situations where it is unclear whether a particular action is appropriate, and within the scope of current job responsibilities, the situation should be discussed with IT management.

16.6 Privileged access user accounts must not be used by individuals for non-privileged day-to-day activities.

16.7 The following constitute inappropriate use of privileged access to council computing resources unless documented and approved by management:

- Avoiding user access controls or any other formal council security controls.
- Avoiding bandwidth limits or any other formal council computing controls.
- Avoiding formal account activation/suspension procedures.
- Avoiding formal account access change request procedures.
- Avoiding any other council procedures that are in written form and/or approved by some level of management.

16.8 The following constitutes inappropriate use of privileged access to council's computing resources under any circumstances, regardless of whether there is management approval:

- Accessing information that is outside the scope of specific job responsibilities
- Exposing or otherwise disclosing information to unauthorised persons
- Using access to satisfy personal curiosity about an individual, system, practice, or other type of entity.

16.9 A user must complete the online request from **Request / Amend Access Form** for a privileged user account and users will have to sign the **Elevated User Permissions Disclaimer Form**.

16.10 The procedures and controls stated in this policy must be applied. In addition, privileged users accounts will be controlled by:

- Enforcing stronger passwords (see the **Password Policy** for more information on password length and complexity)
- Not displaying any previous login information e.g. username.

- Limiting the number of unsuccessful attempts and locking the account if exceeded.

- Password characters obfuscated by special characters.

16.11 This is all covered in detail in the **Password Policy** and should be read in conjunction with this policy.

17 TERMINATION OF USER ACCESS

17.1 When a user transfers to another team or activities are terminated or no longer required, it is the responsibility of that user's manager to request suspension of access rights using the appropriate **Request / Amend Access form** and all authority and access shall be removed.

17.2 When a user either leaves the council or activities are terminated or no longer required, their access to IT facilities and application systems must be suspended at the close of business on the users last working day. This process will be initiated by completion of a **Leaver form** from the user's manager.

17.3 A user's access to IT facilities and application systems may be suspended / disabled immediately if there is a security concern or following a security breach.

17.4 When a user's activities are terminated or no longer required all RBWM equipment shall be returned to IT services

Document Name	**Information technology access security policy**		
Document Author	**Infrastructure security manager**		
Document owner	**Head of HR, corporate projects and IT Services**		
Accessibility			
File location			
Destruction date			
How this document was created	Version 1	**14/06/2012**	**Security manager**
	Version 2	**25/09/2017**	**Security manager**
	Version 3	**25/06/2020**	**Infrastructure security manager**
Circulation restrictions			
Review date	**25/06/2022**		