www.rbwm.gov.uk
Royal Borough of Windsor & Maidenhead

Security Policy
IT ACCESS SECURITY

Introduction
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.

Policy Statement
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.

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.

Not covered by this Policy
Physical access security is not included and has its own policy.

Those Affected
This policy applies to Councillors; employees of the council (including system support staff with privileged access); other organisations; contractual third parties and agents of the council.

Roles and Responsibilities
1. Users of council IT facilities – must comply with the policy rules and procedures.
2. Council Managers and Team Leaders – must ensure their staff comply with the policy and provide advice to them. Must ensure security incidents are raised in response to IT access security concerns or security breaches.
3. The IT Service – 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. The IT Service – ensure that privileged and systems administrator access is strictly controlled based upon valid business justification and specific job requirements.

Policy Compliance
This policy must be complied with. Any breach of the policy could constitute a disciplinary offence. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).
If you do not understand the implications of this policy or how it may apply to you please seek advice from your council manager, the IT Service, or the Information Governance team.

Applying the Policy - Passwords
Passwords are the first line of defence for IT systems and, together with personal user identifiers and IT access codes, establish that people 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 our computers and systems.

<u>Password Strength</u>
A *weak password* is one which is easily discovered, or detected, by people who are

not supposed to know it. Examples of weak passwords include words picked out of a dictionary, names of children and pets, car registration numbers, simple patterns of letters from a computer keyboard, or any variation of the word 'password'.

A *strong password* is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of password hacking software.

Rule 1 Use strong passwords containing a mixture of capital letters, small letters, numbers, and special characters if they are permitted.

Protecting User Identifiers, IT Access Codes and Passwords
It is of utmost importance that these are protected at all times.

Rule 2 Never reveal your log on user identifier(s), IT access codes or passwords to anyone. Do not display them in your work place or elsewhere.

Rule 3 Avoid writing down your user identifier(s), IT access codes or passwords. If you need to write them down keep them out of sight, preferably locked away.

Rule 4 Do not allow others to see you enter the characters or numbers you input when entering your user identifier, access code or password.

Other good practice security advice includes:

- Never use a 'remember identifier or password' function because it makes access less secure.
- Do not use any part of your user identifier within the password.
- Avoid using the same password to access different Council systems.
- Do not use the same password for systems access inside and outside of work.
- Only store your passwords in an electronic file if they are encrypted.

Changing Passwords

Rule 5 Change your passwords regularly (at least every 90 days), or whenever the IT system prompts you to change it.
Rule 6 Any default or temporary passwords must be changed as soon as possible.
Rule 7 If you know or suspect that your password has become known to others, get it changed immediately and report your concern in a security incident report.
Rule 8 Do not re-use the same password.

Applying the Policy – Prevent Unauthorised Access to Information and Systems
Other precautions must be taken to reduce the risk of unauthorised IT access, i.e.

Rule 9 Use password-protected screen savers with time delays to ensure access is denied to others when you leave your computer unattended.
Rule 10 Shut down and switch off computers you use at the end of the working day.
Rule 11 Lock your computer at all times (e.g. by logging out or by using control-alt-delete-space/enter) before leaving it unattended.

Applying the Policy – System Administration Procedures
Use of council computing facilities requires registration and granting of access rights by either (a) IT Services, (b) an approved IT Support service, or (c) by a nominated systems administration role within a council service.

When using the council's IT facilities it is your responsibility to comply with any security conditions and the council's information security policies. You must have

previously confirmed your responsibilities in a signed employment contract, a confidentiality clause, or a security declaration.

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.

Granting of IT access rights will normally be by the provision of a 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.

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

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 documented, secure and auditable.

Applying the Policy – User Access

User access control procedures must be documented, implemented and kept up to date for each IT facility to prevent unauthorised access.

Rule 12 A request for access to council facilities or IT application systems must be submitted for approval by using the appropriate IT access request form. A council manager or team leader must approve the request.

Rule 13 IT users, or their line managers, must notify the IT Service Desk, or responsible council service, of any change in status which may affect their right to use council IT facilities.

The IT access management process extends from the initial registration of new users to the final de-registration of users who no longer require access. Each user must be allocated access rights and permissions that are appropriate for the tasks they perform. They will normally have a unique login and password that is used every time they log on to a system.

Rule 14 User IT access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated.

Rule 15 System IT administration accounts must only be provided to users who are required to perform IT administration tasks in their job role. Administration accounts must be disabled immediately when no longer needed.

<u>User access to Shared (Generic) User Accounts</u>

In exceptional situations a shared (generic) user identifier may be authorised by the IT Service, on receipt of the appropriate authorisation request.
Sharing a user identifier 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.

If a shared user account is approved, the authorising manager will be responsible for the following additional security measures:
(1) Maintenance of an up to date list of who is authorised to use the shared identifier.

(2) Training for users of the shared identifier to ensure they understand the security risks and how to minimise them.
(3) Maintaining an audit trail showing who is using any shared identifiers at any time.

The above security measures may be audited.

Termination of User Access

Rule 16 When a member of staff either leaves the council or transfers to another team, it is the responsibility of that person's council manager to request suspension of access rights using the appropriate IT access request form.

When an employee leaves the council, their access to IT facilities and application systems must be suspended at the close of business on the employee's last working day

Rule 17 Access to IT facilities and application systems may be suspended at any time if there is a security concern, or following a security breach.

IT User Responsibilities

Rule 18 It is a user's responsibility to prevent their log on user identifier and password being used to gain unauthorised access to council systems by following the security rules outlined in this policy.

Rule 19 Any changes to staff roles and access requirements must be communicated by the council manager or team leader to IT Services or an authorised systems administrator.

Rule 20 It is a user's responsibility to ensure that any council laptop or portable computer issued to them is approved by the IT Service and protected by up to date anti-virus software. They must normally do this by physically attaching the portable computer to the council IT network on a regular basis.

Network Access Control

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.

Rule 21 Specific approval must be obtained from the IT Service Desk before connecting any privately owned or equipment from other organisations to the council's network.
Rule 22 Where remote access to the council IT network is required, a request must be made to the IT Service Desk for access authorisation and set-up.
Rule 23 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 the IT Service Desk before first connecting to the council IT network. Access will be logged and may be monitored.

Applying the Policy – Privileged Technical Access

System administrators and IT support staff may require additional privileged 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.

Rule 24 IT Services must ensure that privileged account access is strictly controlled and based upon valid business justification and specific job requirements.

Rule 25 IT Services must monitor access to privileged accounts.

Rule 26 Privileged access user accounts must not be used by individuals for non-privileged day-to-day activities.

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

- Enforcing stronger passwords
- 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.
- Displaying a general warning notice that only authorised users are allowed.

Application Data Access Control
Access to data within IT applications must be restricted using the security features built into the individual IT facility. The business owner of the software application is responsible for ensuring appropriate and secure access to the system.

Related Policies
GCSx Acceptable Usage Policy and Personal Commitment Statement.
Security Incident Reporting Policy.

Related Documents
Terms and Conditions of Employment – this states that employees are required to follow the council's policies, procedures, and guidelines, including those for security.

Related Legal and Regulatory Obligations
UK Data Protection Act
Information Security Management Standard ISO/IEC 27001:2005

Any Other Information
None