Torfaen County Borough Council

Acceptable Use Procedures

Version 4.0 Live

**DOCUMENT CONTROL**

|  |  |
| --- | --- |
| **Title:** | **Acceptable Use Procedures** |
| **Document Owner:** | **Senior Information Risk Owner** (SIRO) |
| **Document Author:** | **Sue Bullock** |
| **Reference:**  | **IG006(A)** | **Retention Period:** | **Until next review** |
| **Document Classification:** | Official | **Location:** | SWOOP |
| **Version / Status:** | 4.0 Live | **Approved by:** | SIRO/Leadership |
| **Current Issue Date:** | January 2022 | **Next Review Date:** | January 2025 |

**REVISION HISTORY**

|  |  |  |  |
| --- | --- | --- | --- |
| **Issue Date** | **Version / Status** | **Reason for Change** | **Changed By:** |
| November 2020 | 1.0 Live | Implementation – Procedure separated from Policy  | Sue Bullock |
| May 2021 | 2.0 Live | Zoom updated –Section 5 | Sharon Clifford |
| June 2021 | 3.0 Live | Webex/webinars added – Section 5 | Sharon Clifford |
| January 2022 | 4.0 Live | 1st Annual Review – changes made to Secure Email facility and O365, BYOD in scope, general grammar changes, accessing software and new template | Sharon Clifford |

**Table of Contents**

[**1.** **PURPOSE** 4](#_Toc89781533)

[**2.** **SCOPE** 4](#_Toc89781534)

[**3.** **AIMS & OBJECTIVES** 4](#_Toc89781535)

[**4.** **RESPONSIBILITIES** 5](#_Toc89781536)

[**Accessing the Council’s Corporate Network** 6](#_Toc89781537)

[**Passwords** 7](#_Toc89781538)

[**Use of Email** 8](#_Toc89781539)

[**Use of Secure Email Accounts** 9](#_Toc89781540)

[**General Use of the Internet** 10](#_Toc89781541)

[**Corporate Internet** 10](#_Toc89781542)

[**Personal Use of Gov Wifi** 12](#_Toc89781543)

[**Security** 12](#_Toc89781544)

[**Data Processing and Reporting Breaches** 13](#_Toc89781545)

[**Social Media and Blogging** 14](#_Toc89781546)

[**Streaming - Music and Video** 15](#_Toc89781547)

[**MICROSOFT Office 365/TEAMS** 15](#_Toc89781548)

[**Handling Personal Information** 17](#_Toc89781549)

[**General** 17](#_Toc89781550)

[**5.** **LEGISLATION & KEY REFERENCE DOCUMENTS** 18](#_Toc89781551)

[**6.** **MONITORING AND REVIEW** 19](#_Toc89781552)

[**7.** **COMPLIANCE** 20](#_Toc89781553)

# **PURPOSE**

Torfaen Council uses a corporate network linked to various systems and equipment throughout departments and the appropriate use of these information/data assets are critical to maintain business and protect the integrity of the Council. As new and emerging technologies become widely available to assist with remote working it is essential that staff recognise possible risks and their responsibilities.

The purpose of this Procedure document, which should be read alongside the Acceptable Use Policy, is to guide and protect you as to what you can and cannot do. It is not exhaustive and if you are unsure as to any aspect you should seek guidance from the Data Protection & Information Governance Team on DPA@torfaen.gov.uk or your departmental Data Protection representative as listed on SWOOP.

# **SCOPE**

This procedure applies to all records created, received, maintained and held in all formats by the Council and applies to:

* All employees, whether office based or working via remote access, including contractors, volunteers, agencies and partner organisations operating on behalf of the Council.
* All elected members whilst working on Council business.
* All equipment that is owned or leased by the Council.
* All resources owned by the Council including corporate information which is held/accessible on personal devices approved through BYOD Policy and Guidance

# **AIMS & OBJECTIVES**

This procedure is applicable and designed to:

* Establish and maintain acceptable working practices to protect the Council and those users carrying out work on its behalf.
* Ensure that all members of staff/elected members and third-party users are aware of and understand their personal responsibilities in the acceptable/non-acceptable use of corporate information and systems/applications controlled by the Council.
* Ensure the confidentiality, integrity and availability of information and systems are adequately protected.
* Enable staff/elected members and all third-party users to utilise the information, equipment and networks appropriately and thereby ensure the Council is not compromised through inappropriate use
* Support, advise and protect staff/elected members and all third-party users from non-compliance and potential disciplinary action.

# **RESPONSIBILITIES**

The following individuals/groups have specific responsibilities:

|  |  |
| --- | --- |
| Senior Information Risk Owner (SIRO) | Overall executive responsibility for the Acceptable Use Procedure and standards and their application throughout the Council |
| Data Protection Officer | To monitor and promote compliance of the Acceptable Use Procedure and report back to the service areas via Leadership Team and the IMGReview, implementation, and governance through the Information Asset Owner’s Group (IAOG) and Information Management Group (IMG) |
| Data Protection and Information Governance Team | Policy formulation and review and providing advice and guidanceEnsuring that the Acceptable Use Procedure are kept up to date and relevant to the needs and obligations of the Council |
| Heads of Service/Line Managers | Ensuring that this Procedural document is made known to all staff, inclusive of agency workers, contractors, volunteers, students or anyone accessing the Council’s systems or information and in doing so ensuring awareness of their responsibilities for acceptable use/actions To assign clear responsibility for information which passes out of their control following (for example) restructuring, moving of functions, closing of projects |
| All staff and elected members | Adherence to the Acceptable Use Procedure and related standards/guidance when managing, storing and disposing of the information they create and receive during the course of their duties To undertake any training/awareness providedTo ensure that the information held by the Council is disposed of appropriately and that all sensitive information is disposed of securelyTo report immediately any observed or suspected incidents where sensitive information has or may have been insecurely disposed ofDocumenting of processes and evaluating procedures within their service areas |
| Systems Administrators | Management of the data systems in their service area in conjunction with SRS technical staff. System-specific procedures should be made available to all staff using specialised service area systems such as (but not limited to) WCCIS/Civica/etc. |
| Shared Resource Service (SRS) | Managing the network infrastructure, ensuring system continuity and security |

Users must at all times comply with the Council’s policies/procedures/guidance and applicable legislation that applies.

Each time you access the Council’s network from a corporate device you will be asked to accept that you have read the Information Security Procedures Statement & Acceptable Use Policy and that you agree to comply with them. In addition, the SIRO may add to these requirements at any time to further secure the Council’s networks and procedures.

Employees should be aware that the Council reserves the right to monitor and access user’s corporate accounts at any time to ensure compliance and mitigate against risk. Any deliberate or malicious use by users of the Council’s assets **may lead** to a disciplinary investigation and further action being taken in accordance with the Council’s Disciplinary Rules and Procedures.

# **Accessing the Council’s Corporate Network**

You will as an employee/user have access to network shared drives such as the M, U and others. The I drive is a private/personal drive and C is a temporary unsecure drive.

When accessing these drives, you **must:**

* Have permission, your Line Manager would have completed a User Access Request (UAR) to allow you to access certain areas of the system to undertake your job.
* Accept and agree the Information Security/ Acceptable Use Statement on the login/splash screen when you first log in and always log in with your own credentials, this will usually be your Payroll number and a password.
* Lock your corporate computer or mobile device when unattended by using the Windows Key  & L or Ctrl, Alt & Delete, & Enter. At the end of the working day you must lock or shut your system down.
* Save (transfer) corporate documents/information to the Council’s shared drives specific to your service area, your manager will inform you which drive to use.
* Only use the I drive for your private use such as storing your own personal information but not media/photos/etc.
* Only use the C drive on an encrypted machine, and with prior approval from your manager, as a temporary measure until you can transfer the file to the relevant corporate drive as it is not backed-up and is not secure
* Report suspected Malware/ransomware/activity of any kind on your device to the SRS Service Desk on 01495 766366. Following, you must power down immediately and unplug your hardwired ethernet cable.
* Ensure your laptop is encrypted and accept SRS updates.

When accessing these drives, you **must not:**

* Share your log in details or allow anyone to use your username and password. Where a shared inbox is required, please contact the SRS Service Desk on 01495 766366 to set up with a UAR completed by your manager
* Access areas in relation to previous roles unless required to do so for business purposes ensuring you have the appropriate authority.
* Breach security by disrupting any network/s, accessing information/systems/networks for which you do not have authorisation or no legal basis to access or access prohibited server/accounts.
* Try to connect any unauthorised device to the corporate network drives, only personal devices that have been approved through the BYOD Policy and Guidance
* Save business information/ personal photos, videos, music, audio, media files to the I drive and only use the C drive on an encrypted machine and with prior approval from your manager, as a temporary measure until you can transfer the file to the relevant corporate drive as it is not backed-up and is not secure
* Save any corporate business documents to the I drive. There are exceptions whereby there is a requirement to do so such as in matters of HR
* Deliberately or with intent, knowingly introduce any form of virus or Malware onto the Council’s servers/networks.
* Use personal accounts for the Council’s Corporate business or to try and access any corporate network drive.

# **Passwords**

When accessing corporate systems, you will be required to enter a complex password in accordance with the Password Policy and Password Construction Procedures. This not only protects the Council and you but is a requirement for the Council to access and comply with the Public Service Network (PSN) security network provided through the Central Government Cabinet Office for all public services. Without PSN accreditation, the Council cannot undertake its business.

You **must:**

* Have a User ID (usually your payroll number) and complex password to connect to the Councils networks and systems.
* Change your password when prompted (usually 90 days but dependent on system), you must be connected to an Ethernet cable when changing.
* Use a strong password that has a minimum 8 characters, combines uppercase, lowercase, numeric & special characters and should not be obvious, an example of a strong password is M4nChe5ter11td#

You **must** **not:**

* Request your Torfaen Account Passwords to never expire
* Share your username/password or ignore password change requests
* Keep generic passwords or use weak passwords e.g. Password1
* Use the same password across multiple systems
* Write your passwords down or store passwords insecurely

# **Use of Email**

Email is critical to the business of the Council and can be monitored as the information contained belongs entirely to the Council as it goes through our network. Please familiarise yourself with the Procedures and Guidelines for the Use of Email and the Email Policy and Procedures. People who have been granted access to our systems will be given a Council email address purely for business purposes use.

When using email, you **must:**

* Only use your corporate email account for the Councils business purposes.
* Use the VPN facility when working remotely to securely log in.
* Only access your Office.com (O365) corporate account using an ‘enrolled’ personal device authorised via the BYOD scheme
* Ensure the email address to which you are sending information is correct by hovering over the address to display it in full.
* Ensure that any email you send on behalf of the Council is professional, appropriate and complies with the Dignity at Work Policy
* Use caution when receiving emails from unknown or unusual email addresses. If you receive a suspect email you must **not** open it and immediately seek advice from the SRS Service Desk on 01495 766366
* Use particular caution with email links as these may contain malware/viruses, hover the mouse over the link to verify the address stated and follow the same process above if you are concerned
* Ensure your email signature is bilingual in Welsh/English and contains contact details to include your email address, and telephone/mobile numbers in line with the corporate standard to meet compliance standards.
* Report email data breaches immediately to the Data Protection & Information Governance Team DPA@torfaen.gov.uk and your line manager/Data Protection Representative.

When using email, you **must** **not:**

* + Send any business emails or attachments from your Council accounts to your own personal accounts e.g. your personal Hotmail/gmail/AOL or other private email domain/accounts as this is corporate data and will contain information that is private, confidential and/or sensitive in nature. This contravenes our security, technical and procedural measures and leaves the Council open to exposure from regulatory bodies such as the Information Commissioners Office (ICO) and also impacts on Business Continuity for the Council.
	+ Try to access your corporate account using a non-corporate/personal device unless it has been authorised via the BYOD scheme
	+ Use your Council email address for personal use. The Council provides a Wi-Fi network (Gov Wifi) should you wish to send personal emails from your personal email account on a personal device.
	+ Send unprofessional, unsolicited or chain emails
	+ Click on any suspicious links as stated above instead contact the SRS Service Desk immediately on 01495 766366
	+ Promote your own or anyone else’s personal business, political or religious interests
	+ Forge or misuse any email header information
	+ Use your corporate signature for non-business emails

# **Use of Secure Email Accounts**

Information sent by the Council via email can be intercepted once it leaves our network and therefore when we send personal information to an individual or organisation, we must make every effort to ensure its security. The Torfaen email system is TLS enabled but you must ensure the recipient is also TLS enabled before sending sensitive information.

If you are sending/replying to a new contact/organisation:

* Check the email address is TLS 1.2 or above by using this email address checker [Check TLS Website](https://www.checktls.com/) and selecting the ‘Show Your SSL Version’ box
* If you still have concerns, contact security@srswales.com to verify the email address is accredited as being secure
* If they are not accredited, you will need to:
	+ use the OneDrive facility, ensuring you protect the data by following the ICT Guidance document

**OR**

* + password protect attachments ensuring no personal information is included within the body of the email
* Generally, email addresses ending .gov.uk/pnn.uk/wales.nhs.uk are secure however you must be cautious as these can be ‘spoofed’ and you should hover over the address to reveal the true sender before replying

If you are sending to an individual with a private email address such as yahoo/AOL/Sky/etc, you must:

* use the OneDrive facility, ensuring you protect the data by following the ICT Guidance document

**OR**

* password protect attachments ensuring no personal information is included within the body of the email

If you receive an email from an organisation that uses Egress:

* You will need to set up an account
* Follow the instruction in the email to access the attachment

# **General Use of the Internet**

The internet is a business-critical tool used by the Council to deliver its daily business.

The Council provides a corporate secure broadband connection called Torfaen Gov Wifi for Council business that users can remotely or hard-wire connect to, when using Council equipment enabling the user to access the corporate network drives and business folders.

The use of this network has a direct impact on the internet speed due to broadband width, therefore it is important that this business tool is used correctly.

The Council reserves the right to monitor Internet usage to include the monitoring of broadband use, access any data that you search, write, send, receive or store, usage while connected to the network or while using VPN. Accessing/Monitoring information will normally occur in consultation with the employee’s line manager and/or HR with reasonable cause.

**NOTE**: **The Council does allow staff/users to access the corporate network for personal use during official breaks and when signed out, such as lunch breaks or at other times if approved by your line manager and subject to certain conditions identified in the following section.**

# **Corporate Internet**

When using the corporate Internet, you **must**:

* Ensure all business documents/information/communication is sent through the corporate network. If the information is of a sensitive nature this should be sent using the OneDrive facility or as a password protected attachment and a separate email sent to the recipient requesting a telephone call to receive the password to open the attachment to avoid business delays.
* Ensure communication and information exchanges directly relate to missions, goals and work tasks of the Council
* Only use for research, advisory, standards analysis and professional society or development activities
* Only order goods or services within the guidelines of the authority’s standing orders.
* Use Office 365 work accounts and other approved SRS accounts where available

When using the corporate Internet, you **must** **not:**

* Try to connect your personal device unless it has been approved via the BYOD Policy and Guidance
* Deliberately download software/malware/viruses or other ware that will disrupt and affect the Council’s business
* Save personal photos, videos, music, audio media files
* Access, write, send, read, receive content considered discriminatory, offensive, obscene, threatening, harassing, intimidating, or disruptive to any person or organisation
* Undertake the following functions/activities (downloading or accessing) including but not exclusive to:

List of Unacceptable Actions

* Any activity which may put the Council at risk
* Offensive, obscene, indecent, racist, sexist or other discriminatory information
* Conducting non approved business
* Illegal activities
* Use of material protected by trade secret
* Unauthorised political activity
* Use of Council logos or trademarks for non-business purposes.
* Activities that knowingly cause congestion/disruption to networks and systems
* Malicious attacks that attempt to harm/destroy systems/data
* Attempting to break through security controls
* Personal use of YouTube, Netflix, TV catch-up channels, other radio/TV subscriptions
* Downloading games/audio midi files
* Intercepting data
* Port or security scanning
* Accessing chat rooms (unless for work purposes)
* Offering of products or services
* Unauthorised use, installation, copying or distribution of copyrighted (including Intellectual property rights), trademarked, or patented material/data/information i.e. without consent
* Downloading software without an appropriate licence
* Making copies of computer software owned or licensed by the Council
* Using services/platforms that offer tools such as surveys/forms (whether a free trial or purchased) unless approved by SRS Security Team/ICT Client Manager
* Installing software onto Torfaen systems without prior written approval from the SRS Security Team/ICT Client Manager
* Releasing personal data without authorisation. Personal data should not be published on the internet unless appropriate authorisation has been granted from the Data Protection Officer/SIRO
* Distributing any ‘pirated material’

# **Personal Use of Gov Wifi**

 When using the SRS Gov Wifi network, you **can:**

* Connect your personal device for non-business purposes
* Search the internet for everyday use including the ordering of goods and services for non-business purposes

When using the SRS Gov Wifi network, you **must not:**

* Access outside of official breaks
* Deliberately download software/malware/viruses or other ware that will disrupt and affect the SRS network
* Save personal photos, videos, music, audio media files
* Access, write, send, read, receive content considered discriminatory, offensive, obscene, threatening, harassing, intimidating, or disruptive to any person or organisation
* Undertake any of the functions/activities (downloading or accessing) including but not exclusive to the List of Unacceptable Actions above

# **Security**

Security of our systems is paramount and significant resource is spent annually to ensure malware, ransomware and other cyber-attacks are identified and managed as quickly as possible in order to continue our business. To enable this to function security is continually monitored and users of our systems are pivotal in supporting the security aspects of our work.

You **must**:

* Report loss/theft of a corporate device or approved BYOD immediately to the SRS Service Desk on 01495 766366
* Report any known/potential security issues to the Security Team via the SRS Service Desk on 01495 766366 this includes your personal device if it has been approved under the BYOD scheme to access corporate data

You **must** **not:**

* Try to connect your personal device unless it has been approved via the BYOD Policy and Guidance
* Ignore security flaws, faults or weaknesses in systems/devices
* Transfer data/information outside of the Council unless you have been given specific authority to do so using the appropriate channels
* Perform changes to IT systems/information
* Purchase any software packages without seeking authorisation from SRS/ICT Client Manager/Data Protection team
* Install any software that has not been approved by the formal SRS process
* Access information, systems, services, applications, servers etc. for any reason other than to complete tasks assigned to you during your job role
* Try to access blocked websites or attempt to circumvent security controls
* Share passwords/PINs/authorisation codes/access cards with any person
* Allow persons not employed by the Council to view information or use devices provided by the Council or its partners without authorisation
* Download Council data/transfer information on termination of employment as this belongs to the Council

# **Data Processing and Reporting Breaches**

The Council is required under the UK General Data Protection Regulation to maintain a record of its processing activities which documents the types of information processed and the reasons for collecting it. Therefore, you must notify the Data Protection & Information Governance Officer with changes to the purposes for which personal information is collected and used and any new requirements. You must also ensure that contractors (working for your service area) meet the standards of the UK General Data Protection Regulations when processing personal information on behalf of the Council.

**You must undertake the mandatory Cardinus e-learning Data Protection Awareness Course annually where your role involves processing any personal information. If you have not undertaken this course you should raise it with your manager and the Data Protection & Information Governance Officer at** **DPA@torfaen.gov.uk**

If you experience a breach/loss of data you must inform your line manager and the Data Protection and Information Governance team at DPA@torfaen.gov.uk immediately.

* You must make every effort to retrieve the information as soon as you are aware of the breach/loss
* Templates and guidance are available on SWOOP and assistance available from the Data Protection and Information Governance Team
* You must **not** contact the ICO directly as notification must be via the Data Protection Officer

For further help with Data Protection issues and your responsibilities as an employee, please refer to the relevant TCBC Policies listed at the end of this Procedure.

# **Social Media and Blogging**

This relates to personal use of online tools, websites and services that share content, profiles, opinions, experiences, interests and media e.g. Facebook, Twitter, Snapchat. Please refer to the Social Media Policy and Guidance document for further clarification.

You **must:**

* Ensure that anything you post is allowed to be in the public domain, distribution of material cannot be controlled once posted
* Be aware of geo-location applications as these reveal your real time location and could display your work address if accessing during lunchbreaks
* Use privacy settings to reduce personal information being accessed by unintended recipients
* Be aware that although Blogging is acceptable it must only be done in a professional manner that will not bring the council into disrepute and is subject to monitoring
* Ensure that any posts from employees to newsgroups contain a disclaimer stating that the views contained are their own and not those of the Council unless for normal business duties

You **must not:**

* Express strong personal views on accounts that identify you as an employee of the Council
* Attribute any personal views to the Council when blogging or using any other forms of social media
* Defame or disparage the Council, its customers, clients, business partners, suppliers, vendors or other stakeholders
* Breach the Council’s Dignity at Work Policy
* Breach the Data Protection Legislation (DPA 2018/ UK GDPR)
* Breach other laws or ethical standards
* Use corporate logos, brand names, slogans or other trademarks, confidential or proprietary information without Council permission

# **Streaming - Music and Video**

* Video and music streaming can be subject to copyright and licence agreements, these must only be used for business purposes/training such as researching video/training on YouTube
* You must not access the following for personal use when connected to the corporate network, YouTube, Netflix, TV catch-up channels, other radio/TV subscriptions, download games/audio midi files

# **MICROSOFT Office 365/TEAMS**

Video Conferencing/Virtual Meetings

* Microsoft Teams is a software application that enables virtual meetings. Training and guidance documents are available through the ICT Training and Support link in SWOOP.
* You must **only** record (audio/visual) meetings/calls where a business need has been identified and approval has been obtained from the ICT Client Manager/Data Protection and Information Governance team.
	+ Once the specific request has been approved you **must:**
* Move the recording from the Chat area, by selecting the download button, it will save to your Downloads folder.
* Then immediately transfer the recording to the relevant Corporate network drive (M) or service area specific systems such as WCCIS/One.
* Be aware that all recordings are corporate business records and therefore form part of Business Continuity, Information Management/Governance and are Auditable records.
* Follow the departmental retention guideline for the specific type of record
* Ensure the record is searchable and available as all recordings are subject to SARs and FOIs. Where redaction is required there must be a suitable method in place to achieve this at service area level.
* Council approved facilities for Video conferencing should **only** be undertaken through Microsoft Teams or SKYPE. Zoom and Webex may only be used under certain circumstances (please see paragraph below). Due to security controls, other video conferencing applications have been deemed unsecure for the Council’s use.
* If you have permission to attend a Webinar, please ensure you follow the guidance in the paragraph below
* Guidance pertinent to homeworking and the COVID19 situation are available in the Information Management section on SWOOP.
* You must not access a meeting via another person’s calendar appointments unless invited or authorised to do so.
* Always exercise caution when receiving an invitation in the same way as if you had received an unsolicited email/link
* Follow the guidance around the Bcc facility when inviting external participants to ensure the security of the meeting

Zoom/Webex or attending a Webinar

Both the Zoom and Webex platforms carry significant risk to the corporate network and as such have strict controls in place which you must adhere to:

You **must:**

* Participate in Zoom/Webex meetings/training or a Webinar, by INVITATION only
* Access only through your work secured browser
* Disclose your name, title and organisation only
* Ensure your privacy by using headphones and apply backgrounds where necessary

You **must not:**

* Host a Zoom/Webex meeting/training or Webinar
* Download the Zoom/Webex or any Webinar Apps from a virtual store
* Share any Council documentation, service user details or personal information
* Disclose any personal/sensitive information in the Chat facility
* Access a Zoom/Webex meeting/training or Webinar through someone else’s calendar
* Remain in the meeting if an uninvited participant is detected – you must leave and wait for the organiser to make contact

Instant Messaging

* Microsoft Chat is an instant messaging facility with a limited retention period
* It must not be used for business purposes or contain personal data therefore you must use an alternative method (such as email)
* All conversations are auditable and subject to FOIs and SARs

Channels

* When using the Teams function you have the option to create Channels and post collaborative documents.
* All posts within a Teams Channel remain for the life of that Team and would need to be included in any SARs/FOIs received.
* The Teams Channel is only a temporary repository and any information needs to be transferred to the Corporate network drive (M) or service area specific systems such as WCCIS/One.
* All Teams Channel posts are corporate business records and therefore form part of Business Continuity, Information Management/Governance and are Auditable records.

# **Handling Personal Information**

As a public body we collect and process personal information on a daily basis, this can be held in electronic, paper or digital format. The main legislation applicable is the Data Protection Act 2018 and the UK General Data Protection Regulations and staff should refer to the Council’s Information Management policies and procedures held on SWOOP.

**General**

* All Council owned devices must be returned upon termination of your employment
* Any Council apps such as Intune Company Portal (MDM) used for accessing the corporate network on your personal devices must be deleted upon termination of your employment.
* No files should be saved to personal devices except in the secure corporate area allocated. These files will be deleted when the app is removed so must be transferred to your team’s work area on the M drive on termination
* You must delete the Intune Company Portal (MDM) app used for accessing the corporate network/information on your personal device if you take your BYOD outside the UK and reinstall it on your return. As stated above this will also delete all files saved in the secure corporate area
* The Council reserves the right to withdraw the ‘personal usage’ facility of Council IT equipment without notice to include personal mobile phones and devices
* Workspaces must be cleared of all items and all sensitive, personal, confidential documents locked away, in line with Alternative Workplace Strategy
* You must only purchase software through the Shared Resource Service and have it installed by SRS employees
* You must not disclose third party information without appropriate legislation/purpose/consent
* **Recruitment** - Persons conducting interviews must arrange to virus check memory sticks and ensure candidates cannot access corporate information/systems
* **Retention** - You must ensure that you only hold the data for the prescribed timeframe as in line with the Retention Guidelines, information for permanent archive should be passed to Gwent Archives and paper files should be passed to the Council’s Offsite Archive Facility for archive until they have reached their deletion date and can be securely and permanently deleted.
* **Disposal** - You must dispose of information appropriately taking into consideration:
* Retention Guidelines
* Information Secure Disposal Policy
* Implications to European funded projects
* Permanent archive
* Insurance purposes
* BYOD Policy and Guidance if you recycle/sell your personal device
* Paper copies have to be securely shredded with facilities being available at all main office areas
* IT equipment needs to be disposed of via the Shared Resource Services and CD’s/USB’s containing personal information must be securely destroyed.
* You must not recycle personal information

**International Transfer** - to comply with the UK General Data Protection Regulations you must implement additional measures if transferring personal data outside of the UK. Therefore, you must liaise with your departmental Data Protection Representatives and the Data Protection & Information Governance Officer.

# **LEGISLATION & KEY REFERENCE DOCUMENTS**

**(Please note this list is not exhaustive)**

The Council will abide by all relevant UK and EU legislation and the following policies and procedures:

* UK General Data Protection Regulation
* The Data Protection Act (2018)
* The Copyright, Designs and patents Act (1988)
* The Computer Misuse Act (1990) / (2011)
* Human Rights Act (1998)
* Regulation of Investigatory Powers Act 2000
* Freedom of Information Act 2000
* Environmental Information Regulations 2004
* Social Services & Well-being (Wales) Act 2014
* Children Act 2004 / 2019
* Equality Act 2010
* Crime and Disorder Act 1998
* Privacy and Electronic Communications (EC Directive) Regulations 2003(amended 2019) PECR
* Welsh Language Standards

###### **TCBC POLICIES**

* Data Protection Policy
* Information Governance Framework
* Information Governance Policy
* Acceptable Use Policy
* Information Security Policy
* Information Sharing Policy
* Records Management Policy
* Retention Policy
* Information Secure Destruction Policy
* Information Access Policy
* Information/Data Loss Policy
* Requests for Information Policy
* Clear Desk Policy
* FOI Policy
* Data Quality Policy
* Password Policy
* BYOD Policy
* Social Media Policy
* Dignity at Work Policy

###### **TCBC PROCEDURES**

###### Data Protection Procedures

###### Offsite Archive & Destruction Procedures

###### Requests for Information Procedures

###### Password Construction Procedures

* + - Retention Schedule (on SWOOP)
		- BYOD Procedures
		- Social Media Guidance
		- Code of Conduct for Employees

# **MONITORING AND REVIEW**

The Information Management Groups are responsible for reviewing the content and ensuring that policies are published on the Information Management site on SWOOP. This Policy will be subject to review when any of the following conditions are met:

###### Content errors or omissions are highlighted.

###### Where another standard/guidance issued conflicts with the information in this policy.

###### An initial 1 year review from policy implementation and on a 3 yearly basis from the current version approval date.

# **COMPLIANCE**

Failure to comply with this procedure may be regarded as misconduct and investigated under the Council’s Disciplinary Rules and Procedures.  In serious cases this may be considered gross misconduct and lead to dismissal from the Council’s employment without notice or payment in lieu of notice.  In serious cases individuals may be liable for prosecution under Data Protection Law