ICT Acceptable Use Policy 2024/25

Contents

Version Control:

Date	Ver.	Author	Comments
August 2008	1.0	ICT	Policy created
March 2009	1.1	ICT	Refreshed and updated
March 2010	1.2	ICT	Refreshed and updated
April 2011	2.0	ICT	Refreshed and updated
Jan 2016	3.0	ICT	Refreshed and updated
August 2017	4.0	Digital Services	Refreshed and updated
April 2018	5.0	Digital Services	Refresh (GDPR)
Nov 2018	6.0	Digital Services	Update following ICT Security policy introduced.
March 2019	7.0	Digital Services	Minor update following the introduction of O365
June 2019	8.0	Digital and Transformation Services	Policy Refresh
March 2020	9.0	Digital and Transformation Services	Policy Refresh and update regarding Messaging Applications
Nov. 2020	10.0	Digital Services	Policy Refresh and update on lost laptops and the use of WhatsApp
Jan. 2022	11.0	Digital Services	Policy Refresh (updated links/email addresses/domains.)
April. 2023	12.0	Digital Services	3.1, 3.1.1, 3.1.2, 8.4.1, 8.5.1, 8.6.2, 8.7.5, 8.10.1, 8.10.2, 8.11.1, 8.12.2, 8.13, 9.1 amended
June 2024	13.0	Digital Services	4.2 and 4.3 added to confirm actions on forwarding emails outside the council.

1. Policy Statement

1.1 The purpose of this policy is to outline the acceptable use of all ICT equipment and facilities within Swansea Council. It is the responsibility of all staff to know these guidelines and to conduct their activities accordingly.

1.2 Inappropriate use exposes the Council to risks including data loss, virus attacks, compromise of network systems and potentially, legal issues. Failure to comply with the policy or abuse of the system may result in facilities being withdrawn and disciplinary action being taken.

1.3 This policy covers all ICT equipment used to conduct Council business including:

- PCs and Laptops
- Internet, email, instant messaging, video conferencing and teams
- Social Media
- Telephones and Fax machines
- Mobile phones

2.0 Scope

2.1 This policy applies to all staff other than those in educational establishments with delegated powers. It also applies to all equipment and systems owned or leased by Swansea Council. The Council will monitor the application of this policy and has discretion to review it at any time through the appropriate consultation mechanisms.

2.2 Whilst the Council wishes to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Swansea Council. Because of the need to protect our network, it may be necessary to scan or monitor information stored on any ICT device belonging to the Council.

2.3 This policy recognises that employees can access the internet, emails and social networking sites via their own personal devices so this policy also covers the employee's use of their personal mobile device / smartphone or any other means of electronic interaction when conducting Council business.

3.0 Using PCs and laptops

3.1 **Data**. Staff must take all necessary steps to prevent unauthorised access to Council data via any Council ICT device. For guidance on data protection, please refer to the data protection policy: https://staffnet.swansea.gov.uk/dataprotectionpolicy

3.1.1 **Accessing data via a Council ICT device**. It is strictly prohibited for staff to access and use Council data of which they are not authorised to view. Any such breaches must be reported to the Council's Data Protection Officer and HR by the relevant manager.

3.1.2 **Private data of staff**. Staff must not save any of their private data (e.g. family photos) on Council devices. This includes the desktop of their laptops/PCs. Any private data that is found on these devices can be deleted without the authorisation of the staff member.

3.2 **Passwords**. Staff must keep passwords for all ICT devices secure at all times and not shared with colleagues. This is to protect unauthorised access to data. For guidelines on passwords, please refer to the **Password Policy** on https://staffnet.swansea.gov.uk/passwordpolicy

3.3 **Screensaver**. All PCs and laptops, must be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes to ensure no unauthorised access. However, staff should lock their device as soon as they leave them unattended using the "Windows" and "L" keys together.

3.4 **Encryption**. To protect Council data, all Council devices must have the latest encryption software installed prior to using them for Council business. This also includes portable data storage systems such as USB sticks and external hard drives. For further guidance on encryption, please refer to the **ICT Security Policy –** https://staffnet.swansea.gov.uk/ictsecuritypolicy

3.5 **Anti-virus**. All devices used by the employee that are connected to the Council Internet/Intranet, whether owned by the employee or the Council, must have approved anti-virus software installed to lower the risk of any malicious attacks.

3.6 **Theft and Security**. Staff who have Council laptops must ensure that they are locked away at the end of the day to lower the risk of potential theft. Managers are responsible for securing laptops where staff are on long-term sick/maternity leave.

3.6.1 Any PCs and laptops used by staff and customers within council buildings must be protected against theft and data loss at all times. All PCs and laptops must be strategically placed so that privacy rights are adhered to and the data presented on screen cannot be read by unauthorised personnel. For further guidance on security, please refer to the **ICT Security Policy -** https://staffnet.swansea.gov.uk/ictsecuritypolicy

3.6.2 When taking laptops **out of the workplace**, they must not be left unattended in shops, pubs, hotel rooms, conference centres and meeting places etc. They must be locked away securely at all times.

3.6.3 Leaving your laptop unattended in **your car** on show throughout the day is not classed as secure. It must be locked away in the boot. Leaving your laptop in your car overnight will not be classed as secure and could also result in possible condensation damage. It must be taken into the house with you.

3.6.4 If a laptop is **lost or stolen**, the relevant staff member must report the incident to their manager, the ICT Service Desk (ict.servicedesk@swansea.gov.uk) and ICT Security officer (cybersecurity@swansea.gov.uk) as soon as possible together with the **asset reference number** of the laptop so it can be disabled straight away. The quicker the laptop can be disabled, the less risk of any data being stolen and less risk of any unauthorised person getting access to our networks.

The Manager will then be sent a security incident form or a breach report to specify how the laptop was lost and what actions were taken to retrieve it. Details of the loss will also be documented by the ICT service desk to reflecting the assets status and lower the risk of any further misuse.

3.7 **Returning a PC/Laptop**. If a staff member leaves the authority, the relevant manager must contact the ICT service desk to either return the equipment or provide details of transferring it to another staff member.

3.8 **Third party use**. Staff must not allow any person not employed by the council, or who is not an elected member, access to or use of council ICT devices, unless the council have given authorisation for the action.

4.0 Using email

4.1 Swansea Council emails with the domain **"swansea.gov.uk"** and **"abertawe.gov.uk"** must only be used for work purposes and not for personal use. The Council reserves the right to monitor staff use of the email facility.

4.2 Staff must not forward any Council emails that contain Council data onto their external personal email account. This will be a breach of our data protection policies and procedures.

4.3 Staff must not create forwarding rules on their email accounts to automatically forward emails outside the Council. This will be a breach of our data protection policies and procedures.

4.4 Occasional reasonable use for personal email accounts can be accessed on the Council network outside work time, i.e. before or after work or during lunchtime, subject to the prior consent of the employees line manager.

4.5 Use of email facility for personal incoming emails is discouraged, although the Council accepts this may be beyond the employee's control. However, if an employee then forwards an inappropriate email using their swansea.gov.uk account, this may be a disciplinary matter.

4.6 Staff must not access or send emails using another employee's user account unless specifically authorised.

4.7 **Email Content Filtering**
The Council will use an email filtering service to prevent the sending and receiving of emails containing:

- known and suspected virus infections;
- keywords, including profane and racist vocabulary;
- attachments whose contents can't be scanned (e.g. encrypted);
- emails from known SPAM mail originators.

4.7.1 The majority of emails found to be in any of the above categories will be automatically blocked or quarantined and a message sent to the relevant staff member to self-assess the content. If the email is legitimate, staff can release the email themselves into their inbox but care should still be taken when opening.

4.7.2 In the event of receiving an inappropriate mail as identified in 4.5 (which has not been quarantined), the "**report message**" icon must be used by staff to report the email as a scam or spam ensuring no attachment or links within the email are clicked on. Once reported, the email will automatically be removed from the inbox.

5.0 Using the internet, instant messaging, video conferencing and Teams

5.1 Staff must not use Council internet, instant messaging, video conferencing and Teams for personal use unless it is used:

- for work related purposes such as research whilst studying for exams;
- for purposes of Helping Hands;
- outside work time, i.e. before or after work or during lunchtime.

5.2 Staff must not access ICT facilities using another employee's user account unless specifically authorised.

5.3 **Monitoring of use**

5.3.1 All information processed on the Council's ICT facilities is the property of Swansea Council and may be accessed or monitored at any time by the Council.

5.3.2 The Council reserves the right to monitor staff use of the Internet, including private use in accordance with this policy. A record of internet sites visited by staff can be accessed by line managers upon request to HR.

5.3.3 If staff receive any inappropriate material or accidentally visit a site that would be deemed unsuitable, make a note of the time and date then contact your line manager who will take the necessary action as advised by HR.

5.3.4 All employees should report any possible misuse of the internet facility to their line manager.

5.4 **Unacceptable use**

5.4.1 The Internet (including emails) should not be used for transmitting or receiving material which is:

- Illegal, obscene, offensive, fraudulent or discriminatory (as defined by the Equality Act);
- Defamatory – including libellous and slanderous comments;
- An intrusion into other people's privacy, or which may be construed as harassing them;
- In breach of copyright (NOTE: it is illegal to download or copy material including images without prior permission of the owner; Furthermore, copyright in material exists automatically, and no statement to this effect is required);
- In contravention of data protection regulations (using data for unauthorised purposes);

5.4.2 Staff must not use the Internet facility (including emails) for:

- Chain letters;
- Private business use or personal advertisements;
- Chat lines or playing games;
- Online betting or gambling;
- Newsgroups, Bulletin Boards, Mailing Lists other than for work purposes, unless in agreement with your line manager – any line manager giving permission for this will need to keep a record of such subscriptions.
- Downloading and sharing software, shareware or Freeware. **Staff are reminded that all software must be installed by Digital Services only**;
- Downloading/streaming of video/audio programs as this can cause network congestion – it should only be done with the authorisation of your line manager and outside general office time when necessary;
- Purchasing online, other than for work purposes, and then only in accordance with Procurement rules and regulations: https://staffnet.swansea.gov.uk/procurementrules
- Circulating pictures, jokes, 'amusing stories', chain letters or inappropriate language that could be interpreted by somebody as discriminatory. NOTE: another person's perception may not be the same as yours. Be aware that any such items could be potentially offensive and may lead to legal action if construed as defamatory or amounting to harassment;
- Making fraudulent offers of products, items, or services originating from any Council account;
- Sending unsolicited messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam);
- Any form of harassment whether through language, frequency, or size.

6.0 Using social media and networking

6.1 Staff and members are not given general access to social networking sites from Council networks. 'Social media' is the term commonly given to websites and online tools which allow users to interact with each other in some way – by sharing information, opinions, knowledge and interests.

6.2 Staff will only be granted access to social media for specific business reasons in a work-related professional capacity. Staff must always use social media / social networking in line with the principles of this policy during working hours or otherwise.

6.3 Outside the Council, staff can freely access social media sites but this must be handled in a sensible and considered way so that neither the individual(s) involved nor the Council is put at potential risk of embarrassment, loss, disciplinary action or criminal proceedings.

6.4 Staff should never publish or disclose any confidential information or information about the Council which is not already in the public arena. Staff must ensure that online activities do not interfere with their job, colleagues or commitments to customers. Staff should not post negative comments about their work, the Council or their colleagues.

6.5 Staff should not post any comments about the Council that do not represent the views of the Council. It is possible that outside activities could lead to complaints of harassment or bullying even though they are not committed in the workplace.

6.6 Staff should not use social media or networking sites to befriend service users or attack or abuse colleagues, customers or suppliers.

6.7 Any abusive or inappropriate comments whether made to or about the Council, colleagues, customers or suppliers will not be tolerated and may lead to legal liability as well as disciplinary action including dismissal.
Also see https://staffnet.swansea.gov.uk/HRsocialmediaguidance

6.8 **Accessing social networking from personal equipment.**
It is a disciplinary offence for an employee to access any form of social networking, email or internet site via their personal mobile or otherwise for personal use during working time. Any employee found to be doing this may be subject to disciplinary proceedings.

7.0 Using desk telephones and fax machines

7.1 Desk telephones and fax machines are at a minimum and are provided for staff to undertake Council duties. They should only be used for personal purposes if the matter is considered urgent. The line manager's permission should always be sought first and calls recorded.

Using mobile phones

8.1 This policy will apply to all Council employees (permanent and temporary) and contractors using or who are provided with a mobile phone to assist them in the performance of their duties or through personal choice.

8.2 The policy is designed to ensure that there are clear internal arrangements for the effective management of mobile phones. Line managers are responsible for ensuring that their staff

are aware of the location of this policy. In addition, line managers are responsible for keeping staff up to date about any changes within the policy.

8.3 The policy ensures that health and safety and lone working issues are identified in relation to the use of mobile phones and ensures compliance with legislation on mobile phones and driving.

8.4 Criteria for Issue of a Council Mobile Phone

8.4.1 Mobile telephones will only be available to staff who have the approval of their line manager, and authorisation of the appropriate Head of Service. Due to costs involved, it must be considered if a basic handset or a smartphone is required. Smartphones should only be issued if there is a genuine need for the role. Anyone with a smartphone must have a Microsoft account licence. An employee will be eligible to have a mobile phone if it is deemed necessary to their position, and they meet any one of the following criteria;

- If the employee's duties require them to spend a substantial amount of time out of the office on work related duties and are considered a mobile worker;
- Staff for whom it is necessary to make essential work related calls off site, as part of their normal course of work;
- Staff who are required to be contactable in an emergency situation, when off-site;
- Staff who are on call after normal business hours;
- Staff identified through the risk assessment procedure;
- Staff who require a phone due to the removal of desk phones and need to regularly contact external people that can't be achieved via another avenue e.g. Microsoft TEAMS or Jabber.

8.5 Pool phones

8.5.1 Mobile telephones may be issued on an individual or on a shared basis i.e. shared phones for people on call. In all cases, it is the line managers responsibility to determine which officers will be part of a shared resource pool, and how this will operate within their area of control. Please ensure that pool phones are highlighted when ordering so as to add an appropriate name to the account. Smartphones will not be issued if required to share as they need to be secured by an individual Microsoft Account.

8.6 Purchase of Mobile Phones

8.6.1 The purchase of mobile telephones must be in compliance with the Council's Procurement Policy and co-ordinated by the ICT Delivery Team.

8.6.2 A mobile phone request can be initiated via the Council's self-service system, the 'ICT Service Desk' portal by the approved administrator for the department. That administrator is responsible for ensuring they have approval to enter into a contract and that all necessary checks have been carried out before the request is placed.

8.6.3 Any requests for a specific model of mobile phone outside the standard phone issued by the Council will be dependent on the user demonstrating the business requirement and this is likely to incur additional charges to the user.

8.6.4 Until such time as mobile phone budgets are centralised, all costs for the purchase of mobile phones will be charged to the appropriate directorate budget. It is the responsibility of each Head of Service to ensure that adequate provision is made in the annual estimates to cover the cost of all mobile phones issued within their directorate.

8.6.5 It is the responsibility of the department administrator to review the usage and billing on the portal of the network provider. Data usage must be monitored along with additional usage charges.

8.6.6 Where a phone contract is renewed and a new upgraded mobile phone is provided, the current handset that is being replaced must be returned to the ICT Delivery Team.

8.7 Rules of mobile phone usage and best practice

8.7.1 Council mobile phones must be on at all times during business or call out hours.

8.7.2 Mobile phones should be kept on silent during meetings/courses etc. to ensure they do not disrupt business.

8.7.3 Confidential information must not be discussed in open areas or inappropriate locations. Many departments/buildings (e.g. hospitals), have local rules regarding the use of mobile phones and these must always be respected. Discretion should be used at all times.

8.7.4 The phone must be returned to their line manager for any periods of extended leave, including maternity.

8.7.5 **Messaging Applications**. The use of certain messaging applications such as WhatsApp or Facebook Messenger is strictly prohibited on council mobile phones except in circumstances when the council consider the use critical for business operations. Although these applications are very useful and let users text, chat, and share media with individuals or groups, they do not protect our data in line with GDPR requirements and therefore must not be used. During certain circumstances e.g. Covid19, access to these apps will be provided however it is strictly on the understanding that no council business is discussed, it is purely to make contact if no other means are available.

8.8 Personal Use of Mobile Phones

8.8.1 Council issued mobile phones are primarily intended for business use only. The current mobile phone tariff is an all-inclusive package for calls and texts, with the exception of some specific numbers (which will incur additional charges to the Council) as detailed on the mobile phone intranet page. https://staffnet.swansea.gov.uk/mobilephoneorders.

8.8.2 Staff must ensure personal use of Council mobile phones is at a minimum with no additional charges incurred. Consistent breaches may result in disciplinary action taking place and the benefit being withdrawn.

8.8.3 Usage of social media and non-Council email for personal use is strictly prohibited on corporate mobile phones.

8.8.4 Line managers and supervisors will monitor usage of Council mobile phones for both private and business use. Private use is at the line manager's discretion however should be kept to a minimum (with no additional charges incurred) and in cases of emergency.

8.9 Lost or Broken Mobile Phones

8.9.1 The Council expects all employees, who have been allocated mobile phones, to take the utmost care and responsibility for them. If a phone is lost or stolen, it should be reported immediately to your line manager and also the ICT delivery team in order to minimise the financial exposure. If it has been set up correctly, the phone can then be securely wiped of any Council data.

8.9.2 If a phone is broken or faulty, please report the fault to the ICT Service Desk and return the faulty handset to the ICT delivery team. A temporary phone may be issued until repair can be affected. If the phone cannot be repaired, a request for a replacement phone will be required.

8.9.3 Depending on the circumstances in which the phone was lost or broken, the Council will be responsible for replacing the phone. However, if carelessness on the part of the employee can be shown as the cause of the loss, the employee will be required to meet the replacement cost.

8.10 Termination of employment

8.10.1 On termination of employment, the employee must remove any google accounts and council data from the mobile phone and return it fully wiped to the ICT delivery team BEFORE they leave. If the line manager has authorised a transfer to a new user the department administrator must contact ICT delivery requesting the change. The new user must ensure that the device is set up using the latest set of instructions found on the Order a mobile phone - Staff portal (swansea.gov.uk). Any accessories supplied by the organisation for use with the mobile phone must also be returned.

8.10.2 Employees who transfer to other departments within the Council and are authorised to have continued use of a Council mobile phone must inform the ICT delivery team via the department administrator in order to update the administrator and budget code information.

8.11 Use of mobile phones whilst travelling abroad

8.11.1 All Council mobile phones/devices will have 'global roaming' disabled by default, meaning that they will not be able to make and receive calls whilst abroad. Should you require any changes to this, it must be requested via the department administrator and authorised by head of service. Access will be given for a set period of time, it will not be permanent.

8.12 Health and Safety aspects of mobile phone use

8.12.1 The Council's Health & Safety team provides advice and guidance on the use of mobile devices in conjunction with the appropriate legislation. Further details can be found on their website. https://staffnet.swansea.gov.uk/healthandsafetyguidancesearch

8.12.2 **Driving and the use of mobile phones.** The Department for Transport has warned that Employers should issue clear guidance about the use of mobile phones and ensure that users are fully aware of the circumstances. In particular, the following points should be noted:

- That it is illegal to use a hand-held mobile phone when driving.
- To use voicemail when driving so that messages can be left
- That a mobile phone should only be used after the driver has stopped in a safe place.
- Avoid taking calls on a hands-free phone, but if the driver must, they should say that they are driving and end the conversation quickly.
- Staff must use their own judgement of the above points with regards to the health, safety and wellbeing of lone workers.

8.12.3 **Swansea Council does not approve of any use of mobile phones whilst driving. This includes making and receiving calls and text messages. Do not make or receive calls whilst driving!**

8.12.4 Drivers are legally obligated to have proper control of their vehicle at all times. The existing maximum penalty for unsafe driving can be an unlimited fine, up to two years in prison, between 3 and 9 penalty points, a discretionary disqualification and an extended re-test.

IF YOU ARE DISQUALIFIED FROM DRIVING, YOUR JOB AND POSITION WITHIN THE LOCAL AUTHORITY MAY BE AFFECTED.

8.12.5 Guidance may be issued to mobile phone users from time to time regarding health and safety in relation to their use, (i.e. Legislation on mobile phones and driving guidance notes, and must be observed at all times).

8.12.6 Staff must ensure that, when they carry a Council mobile phone, they have included in the contacts the number of their line manager and emergency services.

8.12.7 Where identified through risk assessment as a control measure, managers must ensure that a mobile phone is provided. The details of this risk assessment and all control measures must be communicated to the employee. This would include any local level arrangements for lone working and emergencies (i.e. starting and finishing on-site).

8.12.8 Employees are responsible for ensuring that any issued mobile phone is charged and in working order at all times, reporting any defect immediately to their line manager.

8.13 Mobile phone security - passwords

All basic handsets must be set with a PIN code at the very least to ensure security of the contract and costs to the council. Smartphone devices must be set up in accordance to latest procedures which ensure devices are secured via the Microsoft Intune company portal, with PIN codes or biometrics required as part of the setup. Users must have an individual Microsoft account in order to set up and secure the device.

All devices are registered with Samsung which enforce the correct setup and show ownership by Swansea Council. This security allows for the device to be wiped remotely in the event of loss or theft. If a device is lost, this must be reported to the ICT delivery team immediately.

8.14 Publication of mobile phone numbers

8.14.1 Council mobile phone numbers may be published in any of the following locations:

- Business cards
- Email auto-signatures
- Internal council telephone directories
- Council, school and department websites

8.14.2 In certain circumstances a mobile phone user may not want their number published for legitimate reasons. This is decided on a case-by-case basis.

9.0 Reference documentation

9.1 This Policy should be read in conjunction with the following legislation, regulations and Council policies:

- ICT Security Policy
- Data Protection Policy
- Password Policy
- HR social media guidance
- Management of Health & Safety at Work (NI) Regulations 2000
- The Motor Vehicles (Construction and Use) Regulations (NI) 1999 and Road Traffic (NI) Order 1999