Acceptable Usage Policy for email, internet and access to information

Document Control

Version: 3.1	Status: Draft	Author(s): Sarah Davis-Solan
Amendments	2.1 References to GCSX were removed, and advice around email updated 3.0 Policy updated in line with changes to practice and to make the information clearer. Addition of Policy in a Page 3.1 Changes to phrasing throughout to make the document more accessible, and relevant to cyber security requirements, including a new introduction. Removal of specific policy links to reduce need for frequent changes to this document. Wording doesn't reflect any behaviour changes, just aims to make information more relevant and understandable. New Sections are: MFA, Secure Email, Phishing and Spear-Phishing, and ID badges.	
Document objectives: To provide clear guidance on the acceptable use of Wiltshire Council's systems and equipment to ensure good information security		
Intended Recipients: Employees, councillors, contractors, and any third parties who handle paper or electronic data (of which Wiltshire Council is the data controller), or who are users of any of the council's computer systems or equipment.		
Ratifying Body and Date Ratified	Senior Information Risk Owner (SIRO) Information Management Governance Board (previously the IG Board) Unions and Staffing Policy Group for approval	
Date of Issue	Oct 2023	
Review Date	Oct 2028 or when required	
Contact for Review	Information Assurance and Monitoring Lead	
SIRO signature		

Contents

1 Introduction and purpose

The behaviours set out in this policy are designed to not only help Wiltshire Council (the council) comply with data protection laws, but to embed good cyber security practices which will improve our overall cyber security resilience (our ability to protect against potential attacks, or to recover from a successful attack).

Everyone who works for or with the council has a personal responsibility to help protect the confidentiality, integrity, and availability of our information, to enable the council to continue to provide key services to residents. Adhering to these responsibilities and following the guidance will support recovery in the event of a cyber-security attack or other incident.

The aim of this policy is to help people understand how to play their part by only using council information, systems, software and equipment in ways which:

a) Protect council information and equipment from abuse or misuse,

b) Protect the personal information which the council collects, stores, or processes,

c) Help the council to protect against, or recover from, a cyber security attack or other incident.

Understanding and adhering to this policy is a requirement of having access to council information and equipment. Not adhering to this policy may lead to disciplinary action and could result in a referral to the Information Commissioner's Office, or other regulatory body.

The policy sets out individual and organisation-wide responsibilities around information management and governance to enable service areas to work autonomously whilst staying legally compliant.

If you need further information or advice about any topics covered in this policy, please contact the IG team (informationgovernance@wiltshire.gov.uk) who will be happy to assist.

2 Scope

This policy applies to:

a) All employees of the council, and other workers not directly employed by the council (e.g., agency workers, contractors, self-employed consultants, authorised third party suppliers or partners and authorised visitors) who access council information and equipment,

b) The council's ICT infrastructure and estate, both digital and physical,

c) Any device which connects to council networks, including devices authorised under the Bring your own device (BYOD) policy,

d) Any council information, systems, software, hardware, telephony, digital or online services, paper records,

e) Council ID badges.

This policy covers basic principles. Reference should be made to the policies, procedures, and training materials available on the intranet.

2.2 Employee responsibilities

As an employee, you are responsible for reading and adhering to this policy. If you think this policy is not being adhered to, you should notify your line manager. If this is not possible due to the nature of your concern, you should contact the Information Governance (IG) team directly.

You must undertake any Information Governance (IG) related training the council considers necessary to keep your knowledge up to date and to meet our compliance requirements. The mandatory IG e-learning modules must be completed annually, as a minimum.

You are responsible for any information you share, internally or externally. Always follow team, Service or Directorate processes around information sharing. Talk to your line manager if you have concerns about what information is shared, or the ways in which it is shared.

If you think this policy is not being adhered to, you should notify your line manager. If this is not possible due to the nature of your concern, you should contact the IG team directly.

2.3 Line manager responsibilities

As a line manager, you must ensure all employees have read and understood this policy, as soon as possible after joining the council, and before they have access to personal, special category, or confidential information. This applies to temporary or agency employees, or partners, as well as full-time employees.

You should complete all HR processes relating to staffing changes in good time to ensure that employees have the right level of access for their job role. Failure to comply with starter or leaver processes can result in colleagues not having the right access to do their job, or could result in a data breach, should anyone retain access they no longer need.

Make sure all council equipment and ID badges are returned to ICT and FM as soon as they are no longer required.

You must ensure all employees undertake any Information Governance-related training which is made available. If your team require further training, please contact IG.

Ensure all employees understand the risks relating to information security and data protection and know how to report data incidents or breaches in your absence.

If a member of your team believes this policy is not being adhered to, or feels this policy stops them from completing their work, please follow up accordingly, in line with this policy. Contact the IG team for advice or assistance if necessary.

3 Acceptable use

Access to council information and equipment is provided purely to enable employees to conduct the council's business. They are not provided for personal use.

Acceptable use is about behaving in specific ways to ensure the security of council information and equipment.

Do

a) Use council information and equipment appropriately and securely, in line with this policy,

b) Only use council information and equipment to conduct your work,

c) Consider others in line with our Equality, Diversity, and Inclusion Strategy.

Don't

a) Use council information or equipment for inappropriate, offensive, indecent, or unlawful purposes,

b) Use council information or equipment for any personal or private non-council business.

3.2 Monitoring and Auditing

Monitoring and auditing take place to identify and respond to information security risks.

Certain activities, including but not limited to - logging on, sending email, using the internet, and accessing council information - are automatically recorded and may be audited at any time.

These records are routinely monitored to allow us to identify and address activities which might have a negative impact on the council or the people we provide services to, for example a potential data breach where information is being shared non-securely.

If routine monitoring activity identifies any activity which breaches the Acceptable Use Policy, this activity will be followed up and may lead to disciplinary action.

4 Data protection

Personal data is information relating to individuals - including customers, clients, employees and third parties - and is used by the council to provide services to the residents and businesses of Wiltshire.

Data protection laws require that we can demonstrate that we use this type of information fairly and responsibly. The legislation requires us to understand what we collect and use personal data for. We are also required to take “appropriate technical measures" to protect information, when we store it or share it.

Do

a) Ensure personal information is collected only for a specific purpose, and that any personal information we hold is accurate, relevant, held securely, and is not retained for any longer than necessary,

b) Bear in that an individual has a legal right to access their personal information, including what is said about them in emails, Team chats, and other recorded information – even if that information is held on a personal phone or device,

c) Dispose of personal information securely e.g., using the confidential waste bin,

d) Use the IG app to check whether an email domain is secure, before you share personal or special category information you share by email,

e) Minimise, redact, or use a password to protect information you are sharing to a non-secure email address,

f) Check whether we’re allowed to use our information in new ways or for a new purpose before you do so,

g) Read the IG guidance on Data Protection (see Appendix – IG Portal for links).

Don’t

a) Leave your laptop or other device unlocked, when you walk away – even if only for a moment,

b) Let anyone else use your access to information; if they require access, they should request it via official channels,

c) Share any personal information unless there is a clear legal reason to do so. If you’re unsure, check with your line manager prior to sharing.

5 Data Incidents and Data Breaches

A data breach is defined as: a breach of security leading to accidental or unlawful destruction, loss, alteration, unathorised disclosure of, or access to, personal data. This is the case whether the breach is accidental or deliberate.

A data incident (or near miss) happens when there is a security breach, but there is no impact on personal data. Data incidents are how we learn where we need to improve our information security or our cyber security.

All data incidents or breaches must be reported using the IG App, even if you or your line manager thinks they are a near miss. The IG team will support you through responding to the incident or breach, and we'll work with you to look at how to reduce the likelihood of the incident being repeated.

Contact the IG team for advice or if you are unsure how to report an incident.

Data incidents include, but are not limited to:

a) Theft or loss of council information, or equipment which is used to access council information,

b) Accidental or deliberate transfer or disclosure of information to someone who shouldn't have access to it, whether they are internal or external to the council. This includes:

   i. sending an email to - or sharing information with - the wrong person,
   ii. sharing information which you didn't mean to share,
   iii. failing to use BCC when there is a need to keep email addresses private from other recipients,
   iv. failing to protect information when sending it to non-secure addresses (including members of the public),

c) Compromise of login or password for any system used to access or process council information,

d) Any attempt (failed or successful) to gain unauthorised access to council information or systems,

e) Connection of any equipment, hardware, or device other than those provided by, or appropriately approved by, the council,

f) Non-compliance with the acceptable use policy and associated procedures.

Do

a) Report data incidents, without delay, using the IG App (see Appendix – IG App)

a) Read the IG guidance on protecting council information (see Appendix – IG Portal).

5.2 If you think you have a computer virus

ICT use a variety of technical measures to protect against, and detect, viruses or other security issues. However, if you think you have discovered a virus you must immediately:

a) Stop using the laptop or other device and disconnect from the network, either by removing the network cable or by switching off your Wi-Fi connection,

b) Contact the ICT Service Desk without delay to allow any investigation and resolution to take place straight away.

It is better to be vigilant and report something which turns out to be nothing, rather than ignoring something because you're worried you might have it wrong. If you do report in error, you will be treated with respect.

6 Email

Access to council email is provided purely to enable you to carry out council business. When you send emails, you are acting as a representative of the council; defamatory emails, or emails which breach confidentiality can be used in legal proceedings against the council.

Bear in mind that emails, like other work communications, are subject to Data Protection legislation, the Freedom of Information Act and Environmental Information Regulations and could be shared with members of the public.

In the event of a long absence, your email account may be accessed by authorised staff, to ensure business continuity. This access will be strictly controlled and logged.

Email usage is monitored, and your account may be accessed in the event of an investigation or disciplinary procedure, or in response to non-compliance with council policy.

Do

a) Use council email accounts only for work-related activities,

b) Conform to any departmental procedures for the sharing information,

c) Only send personal, special category or otherwise confidential data to an external agency or person if there is a data sharing agreement, partnership working and/or contract in place,

d) Notify your line manager, or an HR advisor, if you receive an email which you believe to be offensive, defamatory, harassing, discriminatory or intimidating,

e) Regularly delete emails you no longer need; retaining email for longer than necessary increases our storage requirements, and creates more work when it comes to responding to requests for information, such as FOI, or Subject Access Requests,

f) Do set an ‘out-of-office’ message if you are going to be out of the office for half a day or longer,

g) Be courteous, polite, and succinct when drafting emails,

h) Go to a council hub if you need to print, it’s not ok to send work home to print.

Don't

i) Use your council email addresses for any personal or private use (personal email sites are accessible via your web browser),

j) Send any council information or work to a personal or private email address to work on, or for your own purposes.

k) Open unexpected attachments or links, and attachments and links from unknown sources,

l) Read other people’s emails without their permission; if you receive an email in error, do not read it. Notify the sender straight away, and then delete the email (the sender is required to report this to IG as a data incident),

m) Auto-forward emails unless you have been authorised to do so by IG. People emailing you directly won’t expect their email to be forwarded, and this may result in a data incident,

n) Create or forward chain letters, spam, jokes, or similar unsolicited emails e.g., hoax virus warning messages,

o) Create, send, or forward email that is offensive, defamatory, harassing, discriminatory, intimidating, or which breaches confidentiality or contract requirements.

6.1 Secure Email

When we send personal or special category information by email, whether it's to a trusted third party, or to a person we are supporting, we're required by law to take appropriate technical steps to protect it.

Many organisations we work with are already on our Secure Email Allow List. This means that ICT have carried out checks on the email address or domain, before setting up a secure email connection.

If an email address is not listed as secure, then will need to take steps to protect the sensitive information you're sharing, such as: password protecting, redacting, or minimising the sensitive information.

Do

a) Use the IG app to check whether an email address is secure before you share information,

b) Take appropriate steps to protect personal or special category information if you're sending it to a non-secure address,

c) Protect sensitive information, even if you're sending it to the person it relates to,

d) Report a data incident to IG if you share information non-securely,

e) Read the IG guidance on Secure Email (see Appendix – IG Portal).

Don't

a) Send personal or sensitive information non-securely. There is a risk that information shared non-securely can be intercepted, and misused.

6.2 Phishing and Spear-Phishing

Phishing is when you receive a fraudulent email, text or message which tries to tempt you to click on a link, or to provide some sensitive info. Very often it's something which sounds too good to be true, such as winning a prize, even though you didn't enter a competition. If it sounds too good to be true it usually is.

Spear phishing messages are more sophisticated and are designed to target a specific person or organisation. These attacks often use a few basic techniques to call you to action. Some spear phishing messages are impossible to spot.

Do

a) Be vigilant. Stop and think before you click:

   i. Check the email address and other details, are they what you'd expect?
   ii. Is this an email you'd expect from that sender?
   iii. Does the email prompt you to take urgent action?
   iv. Does the wording and writing style match what you'd expect?

b) Delete dodgy emails without forwarding or replying, there is no need to inform ICT or IG unless you click on a link or reply to an email,

c) Read the IG guidance on dodgy emails (see Appendix – IG Portal).

Don't

a) Click on links you're unsure of, or not expecting to receive,

b) Reply to, or forward on, dodgy emails. If you need to get advice from someone, you can share your screen.

7 Internet Use

Internet access is provided primarily for official council business. However, at the discretion of your line manager, occasional and reasonable personal use is permitted, if this doesn't interfere with the performance of your duties or the work of others.

a) Certain websites or categories of websites are blocked to protect the user and/or network e.g., gambling sites or pornographic sites,

b) Personal online banking and credit card usage is conducted at your own risk,

c) Personal email sites such as Gmail, Hotmail, Yahoo are accessible.

Do

d) Be responsible and sensible about what you do whilst using council internet access,

e) Close the web browser or tab immediately if you unintentionally access an offensive, obscene, or indecent website, and notify your line manager.

Don't

a) Use council internet access for private business, commercial purposes, or criminal activities,

b) Use council internet access to watch streamed entertainment such as YouTube, Netflix, etc., unless it is for work purposes,

c) Deliberately visit, view, download or circulate material from any website which is offensive, obscene, or indecent e.g., pornographic, sexist, or racist, etc.,

d) Post inappropriate material on the internet,

e) Download or install software, systems, or add-ins without authorisation from IG/ICT,

f) Upload any council information to online storage sites such as Google Drive or Dropbox, or WeTransfer without authorisation from IG.

8 Working remotely and home working

When you work from home, or another remote location, you are still required to adhere to council policy. The requirements around sensitive or private conversations, and locking your phone or laptop are just as important whether you're in the office, in a public area or working from home.

Do

a) Make sure you maintain the confidentiality, integrity and availability of council information, no matter where you work,

b) Read the IG checklist (see Appendix – IG Portal).

Don't

c) Allow anyone to see or overhear council information if they are not entitled to do so.

9 Equipment and Software

Any device or equipment you use to connect to or access council systems or information should be provided by, or approved for use by, ICT, with the exception of devices which are registered as a Bring Your Own Device (BYOD). you wish to use a personal device to access council information, read the Bring Your Own Device (BYOD) policy and talk to your line manager before raising a request with ICT.

This includes cameras, usb storage, pen drives, printers, mobile phones, and CD readers/writers. Any device requiring usb read and/or write access should be requested using the ICT Self Service Portal. Peripherals such as a mouse, keyboard, or headset device will not require approval.

If you believe you require additional hardware or software, talk to your line manager before raising a request via the ICT self-help portal on the intranet.

Do

a) Notify ICT straight away if any device used to access or store council data, is lost or stolen, so they can take steps to protect the council,

b) Agree to any software updates or configuration changes as soon as possible,

c) Lock your laptop or other device if you're going to be away from it,

d) Keep your laptop or other device locked away when not in use, and keep equipment out of sight, where possible, when you transport it off-site,

e) Return any council equipment when you leave the council, or if you no longer use it.

Don't

f) Try to reconfigure any settings on council devices or software,

g) Install additional software on any council device. If you require extra software, talk to your line manager, before contacting ICT,

h) Don't allow anyone other than council ICT staff to connect to or remotely take control of your device,

i) Leave any council equipment in your vehicle overnight.

10 ID Badges

Council ID badges are on show in the Leisure Centres and at main hubs, so that people know who you are. It's important that members of the public know who to speak to, and equally important that colleagues can identify you.

Keeping our ID badges out of sight when we're not at work is one of our first lines of defence.

Do

a) Put your badge when you enter a council building,

b) Remove your badge when you finish for the day, or if you pop out on a break or for lunch,

c) Read the IG checklist (see Appendix – IG Portal).

Don't

a) Wear your badge outside unless you are on council business and there is a requirement to do so,

b) Wear you badge when you are in a vehicle.

c) Let your badge be captured in photographs, not even work ones.

11 Systems Access

You should have appropriate access to all systems and software you require to do your job. If this is not the case, talk to your line manager before contacting ICT or the team responsible for access to that system.

Do

a) Use only your own User ID and password,

b) Keep your passwords secret. If you believe your account or password has been compromised, reset your password and follow the Data Incident Reporting Procedure,

c) Inform your line manager if you have greater access to information than you need to conduct your job,

d) Read the IG checklist (see Appendix – IG Portal).

Don't

a) Share your login details with other people or use anyone else's account. Never allow your account to be used by anyone else,

b) Use an easy to guess or obvious password,

c) Use the same password for work as you use for private purposes,

d) Allow family or friends to use your council equipment when you are working off-site or at home,

e) Try to access systems or data you don't need to conduct your role.

11.1 Multi Factor Authentication

Multi Factor Authentication (MFA) is a way to provide an additional level of security when someone wants to login or access information, by validating that the right person is logging in.

This is sometimes described as getting you to provide "something you know" (your login and password) plus something you're sent (such as a code sent by SMS, or email). MFA can also be achieved by using an application like MS Authenticator.

Where MFA is available, it is strongly recommended that you use it. As cyber security threats continue to increase, it is more likely that council systems, both those developed internally, and those provided by third parties, will require that people be using some form of MFA.

a) To set MFA, employees have the option (in addition to their existing password) to pick one or more of the following methods:

b) App-based authentication (Preferred) – Download an authentication app onto their mobile device.

c) SMS-based authentication – Request an SMS text message to a mobile device

d) Phone Call (landline and mobile) – Request a phone call to a number without an auto attendant, such as a direct dial or landline number.

Where the above methods are not practical, employees should raise with their manager who will discuss alternative access methods with the Information Governance Team.

12 Data Creation and Storage

Always save information to appropriate SharePointOnline sites or relevant line of business software, as required.

If you are working offline, it's ok to temporarily save data locally, but you must move the data to an appropriate location at the earliest opportunity.

Any content created or record, may be subject to various legislation which means it may be shared with members of the public, or on public-facing websites. Make sure you're only creating or recording content for appropriate work reasons.

13 Appendix – IG App

The IG App is provided to enable you to check the Secure Email Allow List or submit new email addresses for checking. The app is also where you need to report data incidents and breaches.

You can either:

a) access the app from the Apps icon on the left-hand side of Teams, or:

b) you can open the app in your browser, using this link.

Either way, you'll be prompted to allow access, so please click through, and allow, as the app requires that access to work.

You can also find the link to Report a Data Incident at the top of the EPIC Hub home page (it will take you to the app), so even if you don't bookmark the app, it's easy to find.

14 Appendix – IG Portal

IG provide lots of information and guidance to supplement this policy.

a) Introduction to the IG App

b) How to use Secure Email

c) Cleansing your data

d) Play your part - and help to keep our information safe

e) Sharing Information securely and password protection

f) Dodgy emails - Phishing and Spear-Phishing

15 Appendix – Associated policies and legal framework

Policies

As well as the Acceptable Use Policy, there are council policies and strategies that set expectations about behaviours and ways of working, which you are required to follow and adhere to.

These documents can be found on the council's Epic Hub intranet pages.

Legal framework

a) Computer Misuse Act 1990

b) General Data Protection Regulation 2018

c) Freedom of Information Act 2000

d) Regulation of Investigatory Powers Act 2000

16 Appendix - Policy in a page

The following list gives a summary of key points from the acceptable usage policy.

a) Keep your login details and passwords private,

b) Never let someone else use your login details,

c) Always wear your ID badge inside council offices,

d) Never wear your ID badge outside,

e) Only ever use council email for work purposes,

f) Regularly delete emails you no longer need; if you need to retain them, save them in the right place,

g) Never send council work files home or to a personal address,

h) Always check whether an email address is secure, before you share personal or sensitive information. If the address is not secure, you will need to password protect, redact, or minimise the information you're sharing,

i) Only share information when there is a legal need to do so – don't overshare,

j) Think before you type, remember - emails, Teams chats, and other any other record may be shared with members of the public under FOI, or SAR,

k) Don't download or try to install software or apps, unless ICT have made them available,

l) Don't use copyright protected images or information.