Information Governance
Acceptable usage policy for email, internet and computer use

Document Control

<table>
<tr><td>Reference Number</td><td>Version 2.1</td><td>Status Published</td><td>Sponsor(s)/Author(s)
Tim Way, Sarah Davis-Solan, David Sausins</td></tr>
<tr><td>Amendments</td><td colspan="3">References to GCSX were removed.</td></tr>
<tr><td colspan="4"><b>Document objectives:</b> To provide clear guidance on the acceptable use of Wiltshire Council’s email, internet and computers.</td></tr>
<tr><td colspan="4"><b>Intended Recipients:</b> Employees, contractors, and third parties who handle any paper or electronic data of which Wiltshire Council is the data controller or are users of any of the council’s computer systems or equipment.</td></tr>
<tr><td colspan="2">Ratifying Body and Date Ratified</td><td colspan="2">Information Governance Programme Board
September 2019</td></tr>
<tr><td colspan="2">Date of Issue</td><td colspan="2">January 2019</td></tr>
<tr><td colspan="2">Review Date</td><td colspan="2">January 2020</td></tr>
<tr><td colspan="2">Contact for Review</td><td colspan="2">Information Governance</td></tr>
<tr><td colspan="2">SIRO signature</td><td colspan="2"></td></tr>
</table>

Associated Documentation
Policies

- Information Security Policy
- Information Governance Policy
- Mobile Working Policy
- Information Incident Management Policy
- Social Media Policy
- Data Incident Reporting Procedures
- Wiltshire Council privacy policy
- Wiltshire Council data protection policy
- Information Governance Communication and Engagement Strategy
- Guidance notes on safe and secure delivery of personal information
- Information Governance Policy
- Records Management Policy
- Bring your own device (BYOD) Policy and Procedure

Legal framework

- Computer Misuse Act 1990
- Copyright Design and Patents Act 1988
- Data Protection Act 1998
- Freedom of Information Act 2000
- Health and Safety at Work Act 1974
- Regulation of Investigatory Powers Act 2000

Contents

1 Introduction

1.1.1 Everyone working for or with Wiltshire Council (the council) has a personal responsibility to safeguard its information assets. This includes using computers, email and provided internet access in acceptable ways to maintain information security.

1.1.2 The aim of this policy is to enable all staff to confidently use the council's computers, email and internet access, and to:

a) prevent abuse or misuse of computer, internet and email facilities;

b) protect users, the council's equipment and the data we hold;

c) ensure compliance with legislation.

1.1.3 Accepting and adhering to this policy is a requirement of using those systems. Not adhering to this policy may lead to disciplinary action.

1.1.4 Council ICT equipment, including hardware, software, mobile devices, email and access to the Internet, is provided to you to enable you to conduct the council's business.

2 Scope

2.1.1 This policy applies to:

a) All employees of the council, elected representatives, other workers who may not be directly employed by the council (e.g. agency workers, contractors, self-employed consultants, authorised 3rd party suppliers and duly authorised visitors) using council-provided credentials and equipment to access or process council information;

b) All the council networks;

c) All devices connected to the council networks, including devices authorised under the Bring your own device (BYOD) policy;

d) Access to council internet and online services.

2.1.2 This policy covers basic principles and reference should be made to the following policies and procedures:

2.2 Employee responsibilities

2.2.1 If you find that this policy is not being adhered to you must inform your line manager. If this is not possible due to the nature of your concern, you should contact the Information Governance (IG) team directly.

2.2.2 You must undertake any Information Security and data protection-related training which the Council considers necessary.

2.2.3 Follow departmental processes for sharing and check the accuracy of what you are doing.

2.3 Line manager responsibilities

2.3.1 You should ensure your staff have read and understood this policy, as soon as possible after joining the council, and before they have access to sensitive or confidential information.

2.3.2 Complete all leaver and new starter processes, and ensure the safe return of council equipment when an employee leaves your team.

2.3.3 If a member of staff tells you that the policy is not being adhered to, or feels that the policy stops them from completing their work, you should follow up accordingly, in line with this policy. Please contact the IG team for assistance if necessary.

2.3.4 Ensure your staff undertake any Information Security and data protection-related training which is made available. Should your team require additional training please contact the IG team.

2.3.5 You should ensure that your staff have appropriate access to all systems required to carry out their role. You should also regularly check that staff do not have too much access, for example being able to read personal or sensitive information which is not necessary to complete their work.

2.3.6 Ensure staff are aware of risks relating to data protection and data breaches or near-misses.

3 Acceptable use

3.1.1 Activity on many council systems and networks is automatically recorded and can be audited at any time.

3.2 Do

a) Use council equipment appropriately and securely, and for the purpose it was provided for.

b) Use the council’s systems appropriately and with consideration for others in line with our dignity at work policy and the behavioural framework.

3.3 Don’t

a) Use council systems for inappropriate, offensive or indecent purposes.

4 Data protection

4.1.1 The council is committed to maintaining high levels of confidentiality and so we must be aware of how we handle personal data. Personal data is the data of customers, clients, employees and third parties, and is used to provide services to the people and businesses of Wiltshire. Personal data should be handled fairly and properly.

4.2 Do

a) Ensure personal data is recorded accurately, is relevant and is not held for longer than necessary;

b) Follow the Guidance notes on safe and secure delivery of personal information;

c) Consider that an individual has a right to access their personal data, including what is said about them in emails;

d) Ensure your portable device is secure, e.g. having a strong password or PIN, and lock the device when not in use;

e) When disposing of personal data ensure it is disposed of securely e.g. using the confidential waste bin;

f) Password protect all information you share by email to any organisation or individual not on the secure email whitelist.

4.3 Don't

a) Leave sensitive data unattended, either on-screen or on your desk;

b) Share any personal data unless there is a clear legal reason to do so. If unsure, check with your line manager.

5 Data Security Incidents

5.1.1 Any data security incident or breach must be reported in line with the Data Incident Reporting Procedure.

5.1.2 Contact the IG team for advice if you are in any doubt about the correct process or procedure that should be followed;

5.1.3 Data security incidents include:

a) Theft or loss of data or any equipment which is used to access council systems;

b) Accidental or deliberate transfer or disclosure of sensitive data to those who are not entitled to receive it, whether internal or external to the council;

c) Any hacking attempts, virus attacks, phishing etc.;

d) Compromise of password for any system used to access or process council information;

e) Any attempt (failed or successful) to gain unauthorised access to data or systems;

f) Connection of any equipment or device other than those owned or appropriately approved by the council;

g) Non-compliance with council information security policies and associated procedures;

5.2 Virus discovery

5.2.1 On discovery of a virus you must immediately:

a) Stop using the device and disconnect from the network, either by removing the network cable or by switching off your wireless connection;

b) Report the virus, or suspected virus, to the ICT Service Desk;

6 Equipment and Software

6.1.1 All equipment must be provided by, or approved for use by, ICT. This includes cameras, memory sticks/pen drives, printers, mobile phones and CD readers/writers.

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

6.1.3 If 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.

6.2 Do

a) Follow the Data Incident Reporting Procedure if you lose or damage any equipment you use to access council data, or if that equipment gets stolen;

b) Agree to any software installation or configuration changes needed to keep council information secure;

c) Lock your laptop if you're going to be away from it.

d) Keep your laptop 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.

6.3 Don't

a) Try to reconfigure any settings on council equipment.

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

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

d) Leave any council equipment in your vehicle overnight.

7 Systems Access

7.1.1 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.

7.2 Do

a) Use only your own User ID and password.

b) Keep your passwords secret, without writing them down. 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 carry out your job.

7.3 Don’t

a) Share your login details with others, or use anyone else’s account. Never allow your user 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 carry out your role.

8 Off-site/Home working

8.1.1 Home Working, and Mobile Working Policies must be adhered to when you are working off-site, or at home.

9 Email

9.1.1 Access to email is provided to enable you to carry out council business.

9.1.2 Defamatory emails, or emails which breach confidentiality can be used in legal proceedings against the council. Bear in mind that emails are subject to both the Data Protection Act, and the Freedom of Information Act, and so may be shared with members of the public.

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

9.1.4 Your email account may also be accessed in the event of a disciplinary, or in response to non-compliance.

9.2 Do

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

b) Conform to any service specific procedures for the transfer of data;

c) Only send sensitive or business confidential data to an external agency or person when you have appropriate data sharing agreement 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) Adhere to good email practice, and regularly delete your old emails, keep any distribution lists up-to-date, and set an 'out-of-office' message if you are going to be out of the office for half a day or longer;

f) Be courteous, polite and succinct when writing emails.

9.3 Don't

a) Use council email addresses for personal use;

b) Email any council data, whether sensitive or not, to personal email addresses, e.g. hotmail, yahoo, gmail, etc. to work on at home;

c) Upload any council data to free internet storage sites such as Google Drive or Dropbox, whether sensitive or not – without authorisation from ICT;

d) Open emails from unknown external senders or click on suspicious links within emails.

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

f) Read other people's emails without their permission; if you receive an email in error, you must not use or disclose any confidential information it contains and you should redirect the message to the correct person;

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

h) Auto-forward emails to any email address unless you have been authorised to do so by the IG team;

i) Send email containing personal information outside the European Economic Area (EEA). If in doubt check with the IG team.

10 Internet Use

10.1.1 Internet access is primarily for official council business.

10.1.2 However, at the discretion of your line manager, occasional and reasonable personal use may be 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.

10.2 Do

a) Be responsible and sensible about what you use the internet for;

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

Don't

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

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

c) Post inappropriate material on the Internet.

d) Download or try to install unauthorised software.

11 Data Creation and Storage

11.1.1 Always save data to appropriate team sites or to your OneDrive.

11.1.2 If you are not connected to the network you can temporarily save data to the local C: drive but you must move the data to an appropriate location at the earliest opportunity.

12 Further information

12.1.1 If you need more information or advice, or have comments about this or any other Information Security related policy, please contact the IG team (informationgovernance@wiltshire.gov.uk) who will be happy to assist.