Wiltshire Council
Where everybody matters

# Wiltshire Council Information Assurance

# Acceptable Usage Policy for email, internet and computer use

This policy can be made available in other languages and formats such as large print and audio on request.

## What is it?

Information, like people, money and tangible assets, is a valuable commodity, and therefore Wiltshire Council takes information security very seriously.

We must and will protect the data we hold relating to members of staff, service users and members of the public, as well as data held for the purpose of providing services to the people and businesses of Wiltshire.

This policy is designed to:

- prevent abuse or misuse of computer, internet and email facilities and paper files;
- to protect users, the council's equipment and the data we hold; and
- to ensure compliance with legislation

This is a high level policy covering basic principles and must be read in conjunction with specific detailed policies if they are relevant to your working practices or system use:

- Information Security Policy
- Protective Marking Policy
- Social Media Policy
- Data Transfer Procedures
- Information Security Incident Reporting Procedures

## Who does it apply to?

This policy applies to employees, elected members, contractors and third parties who handle any paper or electronic data or are users of any of council's computer systems or equipment.

You must read, understand and formally accept this policy before you can use the council's computer systems and equipment.

You will be asked to re-confirm acceptance annually with updates being sent out throughout the year.

## Main points

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

2. You must make sure that at all times you use this equipment appropriately, securely, for the purpose for which it was issued to you without reconfiguration and in compliance with relevant legislation such as the Computer Misuse Act 1990 and Data Protection Act 1998.

3. Use Wiltshire's ICT systems respectfully and not for inappropriate, offensive or indecent purposes; for example do not create, send or forward email that is offensive, defamatory, harassing, discriminatory, intimidating, which breaches confidentiality or contract requirements, or could be described as unsolicited, such as chain letters, spam or jokes.

4. Keep your passwords secret (do not write them down) and do not share them or your login accounts – if you believe your account or password has been compromised, then please reset your password and inform Information Assurance.

5. Be aware that the council monitors email and internet use

**Security Incidents**

6. Security incidents include:

- theft or loss of data or any equipment;
- transfer/disclosure of sensitive data to those who are not entitled to receive it;
- compromised passwords;
- attempt (either failed or successful) to gain unauthorised access to data or systems;
- connection of equipment that has either not been approved by Information Assurance and/or equipment that is not owned by Wiltshire Council;
- non-compliance with Wiltshire information security policies and associated procedures including this policy;
- hacking attempts, virus attacks, phishing etc;

7. If you become aware of a security incident you must follow the procedure outlined in the incident reporting policy ADD LINK.

8. Contact the Information Assurance team and seek advice if you are in any doubt about the correct process or procedure that should be followed;

**Virus Discovery: -**

You must:

9. Immediately report any virus, or suspected virus incidents to the ICT Helpdesk;

10. Stop using the PC/laptop and disconnect from the network by removing the cable at the back of the machine and/or switching off your wireless connection.

11. Secure all media, USB drives and CDs that have been used on the machine and above all do not attempt to ignore or hide the suspected virus infection.

**Systems Access**

You must:

12. Use only your own unique UserID and password. Do not log on as other users.

13. Access only systems or data for which you have both a business requirement and appropriate authorisation.

14. Use Wiltshire Council's systems appropriately and with consideration for others in line with our dignity at work policy.

15. Never allow your user account to be used by anyone else.

16. Never write down or share your password(s) with other users, including IT Help desk staff.

17. Not allow family members or anyone else to use your council equipment when it is in your home.

**Internet Use**

18. You should use the Internet primarily for official council business.

19. You must not use council facilities (including work e-mail addresses) for private business or commercial purposes.
20. Occasional and reasonable personal use is permitted (for example during lunch breaks), as long as this does not interfere with the performance of your duties or the work of other staff. Confirm with your line manager if you are in doubt.

21. You must not deliberately visit, view, download or circulate material from any website which is offensive, obscene or indecent in any way e.g. pornographic, sexist, and racist, etc.

22. If you unintentionally access an offensive, obscene or indecent website you must disconnect from the site immediately and inform Information Assurance.

23. Certain websites or categories of websites will be blocked in order to protect the user and/or network e.g. gambling sites or pornographic sites.

24. Personal online banking and credit card usage is conducted at your own risk.

25. You must not post inappropriate material on the Internet. See the social media and blogging policy for more information.

26. You must not download, install or run unauthorised software (including full products, trial software, games, fonts, shareware, freeware, and screensavers).

**Equipment and Software**

27. You must obtain all of your ICT equipment (hardware/software/devices) via the Wiltshire Council ICT unit and only use Wiltshire Council approved and supplied hardware, software and devices.

28. Do not use your own personal IT equipment to store or process Wiltshire Council data; the only exception is if you are using "GOOD" on a Smart Phone.

29. Screen-lock computers if unattended (by pressing the 'Windows' + 'L' keys simultaneously) and keep laptops and other mobile devices safe.

30. Use only Wiltshire approved and supplied devices, e.g. cameras, secure USB memory sticks (also known as pen drives), printers, mobile phones, etc.

31. Return all ICT equipment to Wiltshire Council ICT unit when it is no longer required, or at the end of your employment.

32. Lock your laptop to the docking station, or store it in a lockable cabinet or drawer when not in use. If you are travelling by car, keep your laptop locked out of sight in the boot, but ensure you do not leave it in there overnight.

**Data Creation and Storage: -**

You must:

33. Always save data onto your network server, and not onto your local C: drive. If you are not connected to the network you can temporarily save data to the local C: drive because they have encryption software installed but you must move the data to a network server at the earliest opportunity.

34. Use the protective marking scheme for processing all council data in electronic or hardcopy; see the "INSERT PROTECTIVE MARKING POLICY" for more information.

**Email and Other Data Transfer Methods: -**

You must:

35. Only send sensitive or business confidential data to an external agency or person when you have a data sharing protocol with the external party.

36. All external email transfers of sensitive information must be password protected or sent via GCSx email; see the data transfer procedure for more information.

37. Conform strictly to the council's data transfer procedures for the movement of large files and information; see the data sharing procedure for more information.

38. Conform to any department specific procedures for the transfer of data.

39. Not email any council data, whether sensitive or not, to 'external' personal email addresses in order to work on it from home, e.g. hotmail, yahoo etc.

40. Not upload any council data to internet storage sites, whether sensitive or not.

41. Not auto-forward emails to any mailboxes unless you have a valid business reason that has been endorsed by Information Assurance - this includes third parties and personal email addresses (hotmail.com etc).

42. Not send email containing personal information outside the European Economic Area (EEA). If in doubt check with the data protection officer;

43. Think before you open emails from unknown external senders or click on suspicious links within emails;

44. Note that in the event of a long absence, sickness and/or a disciplinary or non-compliance issue your manager and other authorised officers will, when necessary, have corporate data forwarded to them from your mailbox; forwarding of such emails will be strictly controlled and logged and the manager will ensure that measures are taken to protect the confidentiality of users' 'personal emails'.

45. Use normal standards of business courtesy when writing emails as with any other communication undertaken on behalf of the council i.e. be courteous, polite and succinct;

46. Consider what you say about other people or organisations; never use aggressive, abusive or deliberately anti-social language and never email hastily in anger;

47. Be aware that legal action may be taken against the council if you send an email which is defamatory or which breaches confidentiality or contract; emails of this kind can be used in litigation or the public's right of access to information under the Data Protection Act 1998 or Freedom of Information Act 2000;

48. Report it to your manager or an HR advisor if you receive an email which you believe to be offensive, defamatory, harassing, discriminatory or intimidating.

49. Adhere to good email practice i.e. regularly delete your old emails, keep distribution lists accurate and up-to-date, and use an 'out-of-office' message if you are going to be out of the office for half a day or longer;

50. Not 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;

51. Not create or forward chain letters, spam, jokes or similar unsolicited emails e.g. hoax virus warning messages.

**Data protection**

You must not:

52. Share personal data about someone without their consent unless it is covered by one of the exemptions in the Data Protection Act 1998. If in doubt check with the data protection officer.

53. Leave sensitive data unattended, either on-screen or on your desk, that may be seen by unauthorised people including paper records or printed information;

## General points

54. Council employees are expected to behave in accordance with the Council's behaviours framework at all times whilst undertaking work for the Council. Further information can be found on HR Direct, from your manager or by contacting an HR advisor.

55. Failure to accept this policy, or if inappropriate use of equipment or data is suspected or discovered, could lead to further investigation.

56. Breach of this policy may lead to disciplinary action which could result in dismissal. Please refer to the disciplinary policy and procedure for more information.

57. Where sanction is necessary with respect to councillors, a complaint may be made against the councillor by an officer under the Member Officer Relations Protocol. This complaint will be heard by the Wiltshire Council Standards Committee as detailed in the Wiltshire Council constitution.

58. No employee will receive less favourable treatment or be disadvantaged by policies, procedures, conditions or requirements which cannot be shown to be justifiable, because they have a protected characteristic. These can include, but are not limited to race, gender, disability, age, sexual orientation, religion or belief, pregnancy and maternity, marriage or civil partnership or gender reassignment

## Employee responsibilities

- You must return any equipment when it is no longer required or your employment ends

- You should inform you line manager if you become aware that this policy is not being adhered to. If this is not appropriate due to the nature of your concern you should contact the Information Assurance team directly.

## Line manager responsibilities

- You should set an example and ensure your staff are adhering to this policy

- ensure all leaver processes for the safe return of equipment are followed if an employee leaves your team

## Further information

If you need any more information or advice, or have comments about this or any other Information Security related policy, then please contact the Information Assurance Team (01225 718863) **add email address** who will be happy to assist.