

Information Systems Acceptable Use Policy

(covers ILT/ICT/IS*)



You are expected to read, understand and sign this policy as a condition of your use of Wiltshire College systems. This policy is in place to protect, students, staff and the reputation of the College. Breach of this policy will be treated as a disciplinary matter.

Wiltshire College is committed to protecting its users and meeting its obligations by ensuring that its information and information processing systems are used in an appropriate manner.

Di Dale
Principal and Chief Executive

The Aims of This Policy...

- To promote the professional, ethical, lawful and productive use of Wiltshire College information systems
- To define and prohibit unacceptable use of Wiltshire College information systems
- To educate users about their Information Security responsibilities
- To describe where, when and why monitoring may take place
- To outline disciplinary procedures

* Please note that there is a Glossary at the end of the document.

1.	Information Security within Wiltshire College	3
2.	General Principles	4
3.	Handling Sensitive Information	5
4.	Your Computer	6
5.	Mobile Devices	7
6.	Your Password	8
7.	E-mail	9
8.	Web Browsing	10
9.	Printing	11
10.	Personal Use	12
11.	Legal Responsibilities	13
12.	Monitoring	14
13.	Enforcement	15
14.	Glossary & Definitions	16
15.	Document Control.....	17
16.	Acceptance	18

1. Information Security within Wiltshire College

Principles of Information Security:-

- Information is an asset. Like any other business asset it has a value and must be protected.
- The systems that enable us to store, process and communicate this information must also be protected.
- 'Information Systems' is the collective term for our information and the systems we use to store, process and communicate it.
- The practice of protecting our information systems is known as 'Information Security'.

Wiltshire College has implemented an 'Information Security Management System' in order to manage and continually improve Information Security over time.

The Information Security Management System (ISMS) is authorised by the governors of Wiltshire College. It is maintained from day to day by the Directors of ILT or ICT.

2. General Principles



Things to know

- ① Information Security is everybody's responsibility.
- ① The college has particular responsibilities to ensure the safety of younger students and vulnerable adults, which govern the implementation of this policy.
- ① Wiltshire College information systems are provided to support college business.
- ① Use of any Wiltshire College information system for personal reasons (including e-mail and the web) is only permitted in accordance with the guidance in this policy.
- ① Wiltshire College monitors many aspects of its information systems in order to protect its lawful interests. Information gathered from such monitoring may be used to instigate or support disciplinary proceedings.
- ① All monitoring is continuous, you should have no expectation of privacy when using Wiltshire College information systems.
- ① All emails and other messages posted on college systems are covered by Wiltshire College's anti-bullying and anti-cyberbullying policies.
- ① If your college work involves use of external systems (such as those of partner organisations) and it appears that such use is in conflict with this policy, advice should be sought from a tutor or line manager.
- ① Breach of this policy will result in disciplinary action. Depending on the severity of the breach, this may also result in:-
 - Criminal proceedings
 - Civil proceedings to recover damages
- ① This policy refers in several places to things that "Others may find offensive". These include but are not limited to:-
 - Pornographic or sexually explicit material
 - Racist, sexist or homophobic material
 - Material that by common social standards would be considered in bad taste e.g. graphic depictions of injury or animal abuse

Things to do

- ☑ Exercise care and common sense in your use of information systems.
- ☑ Report any security-related incident to your line manager or the ICT Helpdesk.
- ☑ Refer to the glossary at the back if you need a definition of any term in this document.

Things not to do

- ☒ Anything illegal.
- ☒ Anything that contravenes this policy.
- ☒ Anything that will harm the commercial interest, reputation or objectives of Wiltshire College.
- ☒ Anything that will potentially harm your employment prospects.

3. Handling Sensitive Information



Things to know

- ① In the course of your work as a student or member of staff, you may come across information of a sensitive nature. This could include:-
 - Personal data relating to living individuals. This is especially sensitive when aggregated to include many individuals
 - Wiltshire College's or third parties Intellectual Property (such as product designs or software source code)
 - Confidential financial information (such as salary or financial planning data)
- ① Sensitive information must be protected against disclosure to unauthorised parties.
- ① It is your responsibility to handle sensitive information appropriately and in accordance with Wiltshire College procedures.
- ① Encryption tools and techniques vary, but all methods can be 'cracked' given sufficient time and resources.

Things to do

- ✔ When creating sensitive information, ensure that it is appropriately marked so that others will know how to handle it, e.g. if it is confidential, mark it "confidential"
- ✔ Communicate sensitive information only to authorised parties using approved methods (described above and below. Such transfers must be authorised by the Data Protection Officer who will provide further guidance).
- ✔ Where encryption is required, use only tools and guidance provided by Wiltshire College for this purpose.
- ✔ Ensure that sensitive information is deleted or destroyed appropriately at the end of its life.

Things not to do

- ✘ Do not send sensitive information via the internet without your tutor's or the Data Protection Officer's approval. Common examples of sending over the internet include:-
 - Using college e-mail to send to external recipients
 - Using web-based e-mail to send to anyone
 - Using instant messaging send to anyone
 - Using file transfer or file sharing web sites
- ✘ Do not copy sensitive data to removable media without your tutor or manager's approval. Common examples of removable media include:-
 - USB sticks and memory cards
 - CDs, DVDs and floppy disks
 - External hard drives and Zip drives
 - Electronic devices with data storage capacity (including phones, cameras, and iPods[™])

4. Your Computer



Things to know

- ① “Your” college computer is the property of Wiltshire College and has been prepared by ICT Services for use on the Wiltshire College network.
- ① Data saved to local (usually C: and T:) drives will not be backed up, and will be lost if your computer breaks, gets stolen or is replaced.
- ① Wiltshire College may at any time and without prior notice:-
 - Audit your computer to ensure compliance with policy
 - Require the return of your computer and any associated equipment

Things to do

- ✓ Log out of your workstation when you are away from it.
- ✓ Save data to your G: drive where it will be automatically backed-up for you.
- ✓ Ensure that files received from anywhere outside the organisation are virus checked before you open them (automatic on college machines). This includes files on removable media. If in doubt, ask the ICT Helpdesk for guidance.
- ✓ If you suspect that you may have a virus, stop using your computer and call the ICT Helpdesk.
- ✓ Ensure that you always shutdown your computer by the approved method to save energy and ensure updates are applied.
- ✓ Ensure that any portable or personal device you connect to the college system is approved for college use. If in doubt, ask the ICT Helpdesk for guidance.

Things not to do

- ✗ Do not allow anyone else to use your computer while you are logged in.
- ✗ Never install software on your computer. This should only be done by ICT Services. Things that you should never attempt to install include but are not limited to:-
 - Screen savers
 - Games
 - Video or audio codecs
 - iTunes or other music download software
 - Instant messaging or communication software (including MSN Messenger, Yahoo Instant Messenger and Skype)
 - Utilities that claim to remove spyware or viruses
 - News readers, ticker-tape services or ‘Gadgets’
- ✗ Do not disable or uninstall any of the software that is installed on your computer

5. Mobile Devices



Things to know

- ① You should read and understand this section even if you do not normally use a mobile device. You may need to do so at some point in the future.
- ① The term 'mobile device' covers any college-owned mobile computing device including:-
 - Laptop or tablet PCs
 - PDAs (also known as Pocket PCs, handhelds or iPaqs)
 - Smartphones and Blackberry e-mail devices
- ① You are responsible for the care and safe storage of any computer equipment that has been issued to you.
- ① If you make use of your own mobile device on college premises you should be aware that this policy still applies.

Things to do

- ✓ Back up your work to the network at regular intervals
- ✓ Always consider the physical security of your mobile device:-

In an unlocked office	Secured with a cable or keep it in a locked drawer
In the car	Concealed from view. Ideally in a locked boot or glove compartment
At home	Ideally within a locked work area. Otherwise within a locked drawer
In a hotel	Concealed from view. Ideally locked in a suitcase
Travelling	Keep the device on your person and out of sight at all times

Things not to do

- ✗ Do not copy sensitive information onto mobile devices.
- ✗ Do not view sensitive information on the train, plane or in any public area. This provides an opportunity for onlookers.
- ✗ Do not allow family, friends or anybody else to use the device.
- ✗ Do not leave mobile devices in the car unless absolutely necessary.

6. Your Password



Things to know

- ① You can change your password at any time (from the CTRL + ALT + DEL menu) not just when the system prompts you.
- ① If you need to grant shared access to files, a diary or e-mail account, this can be arranged by the ICT Helpdesk. You do not need to share passwords.

Things to do

- ✓ Set a password. For main college passwords, the system will ensure the strength of your password. In other cases, you should make it as secure as you can by using some or all of the following techniques:-
 - Use two unrelated words or a short phrase
 - Include at least one number
 - Include at least one upper case character
 - Include at least one symbol
- ✓ Change your password if you suspect that someone else may know it.
- ✓ Writing passwords down is extremely bad practice. If you must do so, observe the following points:-
 - Keep it in your purse or wallet so that it is not left behind when you leave your desk
 - Obscure it in some way so that it is not recognisable as a password
 - Destroy it as soon as you have committed it to memory

Things not to do

- ✗ Do not use one of the 'top 5 predictable passwords':-
 - The name of a family member
 - The name of a pet
 - Your football team
 - A rude word
 - An item or brand name that you can see from your desk
- ✗ Do not disclose your password to anyone. Even ICT Services staff do not need to know it.
- ✗ Do not use anyone else's password.

7. E-mail



Things to know

- ① Wiltshire College e-mail systems are provided for college use. Reasonable personal use is permitted, and is defined later in this policy.
- ① Wiltshire College monitors all e-mail to ensure compliance with policy. This includes email archives.
- ① E-mail is not a secure method of communication. Once a message is sent you have no further control over who reads it.
- ① E-mail is admissible in court and carries the same weight as a letter on company headed paper.

Things to do

- ✔ Use the same care when drafting an e-mail message as you would when writing a letter or memo on company headed paper.
- ✔ Make sure that your message is concise, relevant and sent only to the people that need to read it.
- ✔ Use the telephone or face to face conversation instead of e-mail where this is possible and appropriate.
- ✔ Use your 'Out of Office Assistant' to let people know when you are away.
- ✔ Ensure that forwarding rules are targeted, selective and precise.

Things not to do

- ✘ Never open an attachment that you were not expecting. Even if you know the sender.
- ✘ Never click on a link within an e-mail message unless you know the sender and the purpose of the link.
- ✘ Never supply banking or payment details in response to an e-mail message. This is a well-known method of fraud. Your bank will never request security details by e-mail.
- ✘ Do not send or forward anything that:-
 - Others may find offensive
 - May be defamatory (about an individual or organisation)
 - Is covered by a copyright
- ✘ Do not circulate non work-related material. This includes but is not limited to:-
 - Jokes
 - Chain letters
 - Virus warnings
 - Software
 - Music, pictures or video
- ✘ Never automatically forward sensitive data by the use of forwarding rules.
- ✘ Do not disclose any information about a person that you would object to being disclosed about yourself.
- ✘ Never use e-mail to rebuke, criticise or complain about somebody. You may say something that you regret, and the record will be permanent.

8. Web Browsing



Things to know

- ① Access to the web is provided for college use. Reasonable personal use is permitted, and is defined later in this policy.
- ① Wiltshire College monitors and records all web browsing to ensure compliance with policy.
- ① Access to certain web sites may be blocked in order to protect you and the college. This does not imply the suitability of sites that are not blocked. You must always use your discretion along with the guidance below when visiting web sites.

Things to do

- ✓ Inform the ICT Helpdesk if access to a legitimate and college work-related web site is blocked.
- ✓ Inform the ICT Helpdesk if you believe you have a virus or spyware infection on your computer. This is a routine occurrence; it does not indicate irresponsible browsing, and you will not be disciplined. Do not attempt to remedy the infection yourself.

Things not to do

- ✗ Do not view or download anything that others may find offensive.
- ✗ Do not download anything that is likely to be covered by copyright. This includes, but is not limited to:-
 - Music
 - Pictures
 - Software
- ✗ Do not visit the “high-risk” site categories shown below. Although their content appears to be free, it is often funded by installing spyware on your computer.
 - Free screensavers and smileys
 - Free music downloads or ringtones
 - Free software and serial numbers (also known as warez and cracks)
 - Adult material

9. Printing



Things to know

- ① Colour printers cost much more per page than black and white ones, even if there is no colour on the page.
- ① Printers are provided for college use only.

Things to do

- ✓ Be selective about what you print. Print only when necessary and only the necessary pages of a document.
- ✓ Print double sided to save paper where possible
- ✓ Observe published print procedures and guidance.
- ✓ Keep the area around printers tidy

Things not to do

- ✗ Do not print to a colour printer unless colour conveys important information in your document that would be lost in black and white.
- ✗ Do not resend your print job if nothing happens. Instead, check the following (using guidance in the IT Help system where needed):-
 - Is the print job still listed in the queue?
 - Did you send it to the right printer?
 - Is the printer switched on?
 - Is the printer in an error state because:-
 - There is paper jam
 - It is out of paper
 - It is out of toner or ink



10. Personal Use

Wiltshire College recognises that personal access to e-mail and the web at college helps students and staff to maintain a positive college work life balance.

Limited and 'reasonable' personal use of e-mail and the web is permitted. Reasonable use is defined below. Personal use of all other systems is prohibited.

E-mail and web access for personal use have been provided at considerable risk and cost to the organisation. Wiltshire College asks that students and staff make sensible and conscientious use of these facilities in return.

The web has the power to distract even the most conscientious person. It is easy to spend more time than you intend to on 'addictive' sites like auctions, gaming, social networking and blogging.

All e-mail and web access is monitored to ensure compliance with policy. Students and staff that choose to make personal use of college systems do so in acceptance of the monitoring measures outlined in this policy.

Personal use of these systems is a privilege. Wiltshire College reserves the right to withdraw it either individually or globally at any time without notice or explanation.

Reasonable Use

Reasonable personal use of college systems is that which:-

- Is lawful and ethical.
- Is in accordance with this policy.
- Takes place during authorised breaks or outside of your working hours.
- Does not adversely affect your productivity.
- Does not make unreasonable use of limited college resources.

Unreasonable Use

Unreasonable personal use of college systems includes but is not limited to:-

- Contravention of this policy in any way, including but not limited to the sending, viewing or downloading of:-
 - Material that others may find offensive
 - Unauthorised software
 - Material covered by copyright, such as music, videos or games
- Personal use that can reasonably be described as excessive within the context of a learning or professional working environment.
- Activities for personal financial gain or for business other than that of Wiltshire College and its associated businesses.



11. Legal Responsibilities

Things to know

- ① You are personally responsible for ensuring that your use of information systems is lawful. Failure to do so may result in any or all of the following:-
 - You being personally liable to criminal prosecution.
 - You being personally sued for damages in a civil court.
 - Wiltshire College governors and staff being personally liable to criminal prosecution.
 - Wiltshire College being sued for damages in a civil court.

Things to do

- ✓ Comply with software licences, copyrights and all other laws governing intellectual property.
- ✓ If you process personal data (data that identifies a living individual) in the course of your college work, you must do this in accordance with the Data Protection Act 1998. Your tutor or line manager can provide you with specific guidance on The Act.
- ✓ If you process card payments in the course of your work, you must do this in accordance with the Payment Card Industry Data Security Standard (PCI DSS). Your line manager can provide you with job-specific guidance on handling payment card data.

Things not to do

- ✗ Do not copy college software for use at home or elsewhere.
- ✗ Do not write or say anything defamatory or potentially libellous about another individual or company.

12. Monitoring



Wiltshire College owns the organisation's information systems and any information that resides on them. It reserves the right to monitor any organisational system at any time.

You should have no expectation of privacy when using Wiltshire College information systems, whether for college or personal use.

Monitoring of systems is carried out in order to:-

- Detect and prevent unlawful use of systems
- Detect and prevent misuse of college systems
- Maintain the effective operation of systems
- Protect the reputation of Wiltshire College
- Protect Wiltshire College from legal liability

Raw monitoring data will be viewed and analysed only by the Director of ICT Services and his or her nominated representatives.

On instruction of the Director of ICT Services, the data may be passed as necessary to any of the following:-

- Senior staff as part of the student disciplinary procedure
- The Director of Human Resources
- The appropriate line manager
- The Police

13. Enforcement

Breach of this policy will invoke the college's disciplinary processes.

Serious or persistent breaches may constitute gross misconduct and result in dismissal or suspension.

14. Glossary & Definitions

Chain letters	These are e-mail messages or slideshows that encourage you to 'pass this on to all your friends' or 'pass this on to six people today'
Codec	Software required to run specific video or audio files
CTRL + ALT + DEL	<p>Pronounced as Control Alt Delete, this abbreviation represents pressing all three of the CTRL, ALT and DELETE keys simultaneously.</p> <p>Using CTRL + ALT + DEL when you are logged in will display a menu on the screen. Options include:-</p> <ul style="list-style-type: none"> • Lock Computer (to prevent unauthorised access) • Change Password
Home drive	An area on the college's server that is set aside exclusively for your work. It appears on your computer as a drive letter (usually H:)
ICT	Information & Communications Technology – such as computers, the Internet, mobile communications, e-mail.
ILT	Information & Learning Technology – the use of computers & communications technology for learning & teaching.
IS	Information Systems – used here to cover ICT, ILT & in its more specific sense of management information systems, including information security.
Sensitive	<p>The meaning of sensitive in this context is provided by the Data Protection Act, 1998, Part 1, Preliminary, item 2:</p> <p>“Sensitive personal data</p> <p>In this Act “sensitive personal data” means personal data consisting of information as to—</p> <p>(a) the racial or ethnic origin of the data subject,</p> <p>(b) his political opinions,</p> <p>(c) his religious beliefs or other beliefs of a similar nature,</p> <p>(d) whether he is a member of a trade union (within the meaning of the [1992 c. 52.] Trade Union and Labour Relations (Consolidation) Act 1992),</p> <p>(e) his physical or mental health or condition,</p> <p>(f) his sexual life,</p> <p>(g) the commission or alleged commission by him of any offence, or</p> <p>(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.”</p>
Software	Any program that can be installed on your computer. Examples

	include:- <ul style="list-style-type: none"> • Microsoft Word • An Antivirus program • A game • A screensaver
Spyware	Unwanted software that delivers unsolicited advertising or steals information from your computer. Often bundled with 'wanted' software like screen savers.
User	Any user granted access to Wiltshire College information systems. Including:- <ul style="list-style-type: none"> • Students • Employees • Temporary staff • Voluntary staff • Employees of partner organisations • Contractors and subcontractors • Agents • Work experience placements
You	You are defined as a user of Wiltshire College information systems

15. Document Control

Document Information

Document Title	Information Systems Acceptable Use Policy
Version	2.3
Status	Published policy for students, awaiting further consultation with JCG for staff use.
First Issued	July 2010
EDI assessed	Jude Smith Rachele 16/6/10
Maintained by	Directors of ILT or ICT

Revision History

Version	Date	Details
1.0	Aug 08	policy template before customisation
1.1	May 2010	Draft customisation for Wiltshire College
1.2	June 2010	Amendments by ICT Strategy Group
2.2	June 2010	Amendments following EDI assessment to Draft
2.3	July	Amendments following review by Joint Consultative Group

16. Acceptance

If you do not understand or are unhappy with any part of this policy, please raise this with your tutor or manager or the Directors of ILT or ICT.

Students

Acceptance is electronic as part of your account activation and induction process.

New Staff

You will have received a copy of this policy as part of the information sent to you with your 'Offer Letter'. Your signed copy of the Induction Checklist constitutes your acceptance of this policy.

All Users

Periodically, you will need to re-confirm your acceptance of this policy. During your use of the College network, you will be presented with a process to permit you to indicate your continued acceptance. This process will be entirely electronic.

Thank you.