Information Systems Acceptable Use Policy

(covers LT/ICT/MIS)

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

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

Amanda Burnside
Principal & Chief Executive, Wiltshire College

The Aims of This Policy…

- To promote the professional, ethical, lawful & productive use of Wiltshire College information systems and the British Values of Respect, the Rule of Law and Individual Liberty and Democracy
- To define & prohibit unacceptable use of Wiltshire College information systems
- To educate users about their Information Security responsibilities
- To describe where, when & why monitoring may take place
- To outline disciplinary procedures
- It is intended that this policy is fair to all. Where any part could potentially lead to unequal outcomes, the policy then justifies why this is a proportionate means of achieving a legitimate aim.

Appendix

1. Information Security within Wiltshire College

Principles of Information Security:-

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

2. General Principles

Things to know

- ⓘ Information Security is everybody's responsibility.
- ⓘ The college has particular responsibilities to ensure the safety of younger students & vulnerable adults, which govern the implementation of this policy.
- ⓘ The College has particular responsibility to have due regard for the need to prevent young people being drawn into radicalisation or extremism.
- ⓘ Wiltshire College information systems are provided to support college business.
- ⓘ Use of any Wiltshire College information system for personal reasons (including e-mail & the web) is only permitted in accordance with the guidance in this policy.
- ⓘ 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.
- ⓘ All monitoring is continuous; you should have no expectation of privacy when using Wiltshire College information systems.
- ⓘ All emails & other messages posted on college systems are covered by Wiltshire College's anti-bullying & anti-cyberbullying policies.
- ⓘ If your college work involves use of external systems (such as those of partner organisations, including cloud storage) & it appears that such use is in conflict with this policy, advice should be sought from a tutor or line manager.
- ⓘ Anything you prepare, store, transmit or publish via any of the college's ICT systems could be subject to copyright or intellectual property law.
- ⓘ Careful use of the Internet & other systems will help you to avoid mistakes that could lead to plagiarism & infringement of college academic standards.
- ⓘ 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
- ⓘ 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
    - Extremist or radical views /materials

Things to do

- ☑ Exercise care & common sense in your use of information systems.
- ☑ Report anything you believe to be illegal or any security-related incident to your tutor, 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.
- ☒ Anything that may lead to the display of extremist materials /views

3. Handling Sensitive Information

Things to know

- ⓘ 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)
- ⓘ Sensitive information must be protected against disclosure to unauthorised parties.
- ⓘ It is your responsibility to handle sensitive information appropriately & in accordance with Wiltshire College procedures.
- ⓘ Encryption tools & techniques vary, but all methods can be 'cracked' given sufficient time & 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 & below. Such transfers must be authorised by the Data Protection Officer who will provide further guidance).
- ☑ Where encryption is required, use only tools & guidance provided by Wiltshire College for this purpose.
- ☑ Ensure that sensitive information is deleted or destroyed appropriately at the end of its life (for more information, please contact the Data Protection Officer).

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
  - Using cloud storage or cloud based systems
- ☒ Do not copy sensitive data to any mobile device or removable media without your tutor or manager's approval. Common examples of removable media include:-
  - USB sticks & memory cards
  - CDs, DVDs & floppy disks
  - External hard drives & Zip drives
  - Electronic devices with data storage capacity (including phones, cameras, & iPods^{tm})

4. Your Computer

Things to know

- ⓘ "Your" college computer is the property of Wiltshire College & has been prepared by ICT Services for use on the Wiltshire College network.
- ⓘ Data saved to local (usually C: & T:) drives will not be backed up, & will be lost if your computer breaks, gets stolen or is replaced.
- ⓘ Wiltshire College may at any time & without prior notice:-
  - Audit your computer to ensure compliance with policy
  - Require the return of your computer & 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 & call the ICT Helpdesk.
- ☑ Ensure that you always shutdown your computer by the approved method to save energy & 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 & 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

- ⓘ You should read & 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.
- ⓘ The term 'mobile device' covers any portable device, often incorporating memory, storage and connectivity. Examples include:-
  - Tablet computers, netbooks, laptops and eReaders
  - Smartphones & Blackberry devices
  - PDAs (also known as Pocket PCs, handhelds or iPaqs)
  - Other specialist devices such as cameras, audio & video recorders etc
- ⓘ You are responsible for the care & safe storage of any mobile device which has been issued or loaned to you.
- ⓘ If you make use of your own mobile device for college purposes you should be aware that this policy still applies. Similarly, if you remotely connect to college systems from fixed devices, such as a home computer, this policy still applies.
- ⓘ A further section of the AUP contains additional guidance on the use of **your own** device when using College systems (BYOD).

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 & 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 Identity / Password

Things to know

- ⓘ Students and staff are issued a network login and an ID Badge.
- ⓘ Your Login, Password and ID Badge will control access to College resources.
- ⓘ You can change your password at any time (from the CRTL + ALT + DEL menu) not just when the system prompts you.
- ⓘ 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

- ☑ Comply with rules for the carrying and display of ID. Store it safely when you aren't wearing it.
- ☑ If you lose your badge, report the loss **immediately** to any Reception, LRC or IT Support.
- ☑ 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 at least 6 characters and all of the following: -
  - upper case characters
  - lower case characters
  - numbers
- ☑ 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 give your network login or ID Badge to anyone else.
- ☒ Do not use anyone else's login, ID Badge or password.

7. E-mail

Things to know

- ⓘ Wiltshire College e-mail systems are provided for college use. Reasonable personal use is permitted, & is defined later in this policy.
- ⓘ Wiltshire College monitors all e-mail to ensure compliance with policy. This includes email archives.
- ⓘ E-mail is not a secure method of communication. Once a message is sent you have no further control over who reads it.
- ⓘ E-mail is admissible in court & 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 & 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 & appropriate.
- ☑ Use your 'Out of Office Assistant' to let people know when you are away.
- ☑ Ensure that forwarding rules are targeted, selective & precise.
- ☑ Ensure your emails comply with the Email and Internet Additional Guidance at Appendix A.

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 & 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)
  - Where copyright might be infringed
- ☒ Do not circulate non work-related material. This includes but is not limited to:-
  - Jokes or 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, & the record will be permanent.

8. Web Browsing

Things to know

- ⓘ Access to the web is provided for college use. Reasonable personal use is permitted, & is defined later in this policy.
- ⓘ Wiltshire College monitors & records all web browsing to ensure compliance with policy.
- ⓘ Access to certain web sites may be blocked in order to protect you & 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 & 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, & you will not be disciplined. Do not attempt to remedy the infection yourself.
- ☑ When accessing the internet ensure you comply with the Email and Internet Additional Guidance at Appendix A.

Things not to do

- ☒ Do not view or download anything that others may find offensive.
- ☒ Do not download anything that is likely to infringe 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 & smileys
  - Free music downloads or ringtones
  - Free software & serial numbers (also known as warez & cracks)
  - Adult material.

9. Printing

Things to know

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

Things to do

- ☑ Be selective about what you print. Print only when necessary & only the necessary pages of a document.
- ☑ Print double sided to save paper where possible
- ☑ Observe published print procedures & 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 & 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 & the web at college helps students & staff to maintain a positive college work life balance.

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

E-mail & web access for personal use have been provided at considerable risk & cost to the organisation. Wiltshire College asks that students & staff make sensible & 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 & blogging.

All e-mail & web access is monitored to ensure compliance with policy. Students & 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 & 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 which may infringe 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.
- ☒ Accessing any college system/data (except email and web) for personal reasons, either for yourself or on behalf of others. This would also breach the Data Protection Act 1998.
- ☒ Activities for personal financial gain or for business other than that of Wiltshire College & its associated businesses.

11. Legal Responsibilities

Things to know

ⓘ 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 & staff being personally liable to criminal prosecution.
- Wiltshire College being sued for damages in a civil court.

Things to do

☑ Comply with software licences, copyright & all other laws governing intellectual property.

☑ If you access or 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.

☒ Do not use any college system to access college data outside the scope of your normal job role.

12. Monitoring

Wiltshire College owns the organisation's information systems & 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 & prevent unlawful use of systems
- Detect & 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 & analysed only by the Director of ICT Services & 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 Assistant Principal Human Resources
- The appropriate line manager
- The Police

13. ResNet Service

Overview

In order to comply with safeguarding requirements, the College provides only FILTERED internet access throughout its campuses. This means that access to sites deemed unsuitable for young persons or vulnerable adults are blocked. These sites will include social networking, blogging sites, chat rooms/services etc.

We recognise that those who reside in our Halls of Residence may wish to use such services to maintain contact with family and friends. To meet this need, we offer a 'wired' service, ResNet, which comes in two forms, ResNetStd and ResNetPlus. If you are aged 13 and over and your accommodation is equipped with a ResNet outlet, ResNetStd delivers the standard FILTERED service. ResNetPlus offers an extended, almost UNFILTERED internet access to those who can meet the following criteria:-

- You must be at least 18 years of age
- You must not be classed as a vulnerable adult or in any other 'at risk' group

Additional Conditions of Use – ResNet

You may apply for a ResNet connection via your Accommodation Office who will arrange connection subject to the following conditions:-

The Information Systems Acceptable Use Policy (AuP) applies to your use of all College services including ResNet. The following are additional conditions related specifically to the ResNet service.

- The ResNet service is provided for your sole use. You must not make it available to ANYONE else.
- IP Addresses are issued automatically via DHCP – no other addresses should be configured. The DHCP service will issue addresses for up to 4 devices.
- This is a 'wired' service ONLY. You may install a personal switch to support multiple devices but you must not connect any form of wireless access point or any other device intended to provide remote or shared services.
- Users are responsible for the security and configuration of their own equipment. You must ensure that your devices have the latest available OS updates and that they have appropriate anti-virus protection.
- You connect devices to ResNet at your own risk and you are responsible for all configuration of your devices. The College will provide general configuration information in document form but if a technician is required to attend, a charge will be made.
- You have no authority to commit the College to any charges related to your use of the ResNet service – you are personally responsible for such charges however they may arise.
- The use of any type of port scanner will be regarded as an attempt to gain unauthorised access to machines, and will be considered a breach of the AuP.
- The College reserves the right to suspend access to ResNet where these conditions are not adhered to.
- In the case where ResNet is withdrawn from a user, either permanently or temporarily, due to breach of any of the regulations, no refunds of any kind will be made.
- Moderate use of the network for recreational purposes is permitted, provided excessive network traffic does not result.
- The College reserves the right to FILTER or FIREWALL sites and services as deemed appropriate.
- Usually ResNet access will be enabled on a same day basis but may take longer at peak times.
- The College cannot guarantee a minimum available bandwidth nor continuity of service. In the event of service failure, the College will rectify the problem as soon as possible however

events occurring outside normal business hours and during holiday periods will take longer to resolve.

- All communication will be via College email accounts.

.

14. Using Your Own Equipment on the Network (BYOD)

Things to know

- ⓘ This section of the Acceptable Use Policy describes key requirements for use of any device you own (e.g. tablet, laptop, mobile phone) on college premises & using college infrastructure.
- ⓘ In using your own device at college, you are accepting this policy.
- ⓘ The College cannot allow electrically unsafe devices to use its premises &, from time to time, may test devices brought in by users.
- ⓘ The College cannot accept responsibility for the security, safety or operation of your own device. You must, therefore, familiarise yourself sufficiently to manage your device securely & safely.
- ⓘ When connecting to the college network, a limited degree of scanning for security reasons is required. Additionally, in exceptional circumstances, the College may require access to staff-owned devices in order to retrieve college-related data or information (which remains the property of the College). The latter includes, but is not limited to, responding to Freedom of Information requests.
- ⓘ You may connect the power cord of your device to college power sockets provided that this is for short periods & that you consider other users' needs for access.
- ⓘ It remains your responsibility to keep your device secure.
- ⓘ Where you use your own device, the College does not guarantee that you will be able to use every online or networked facility it provides to its own equipment (one reason for this is that you may have non-standard or unsupported software and operating systems).
- ⓘ The College reserves the right to prevent access by specific devices to college systems.

Things to do

- ☑ Ensure your device is safe to use:
  - Ask yourself if it appears electrically safe – there should be no loose components or worn cables, for example.
  - Any equipment linked to your device is used in a way that protects other people's safety (there should be no trailing cables & kit should not block access, for example).
  - If you see any other person's equipment that appears to be unsafe you should bring this to the attention of appropriate staff.
- ☑ Ensure your device is secure:
  - The machine must be password protected. If you should lose your device, you must change all college-related passwords at the earliest possible opportunity (you are advised to do the same for personal systems accessed from the device). You should also inform ICT Services of the loss; students can do this via their tutor.
  - Anti-virus software is installed & is up to date.

- Updates related to the security of software & operating systems on your device are kept up to date.
- You have securely marked your device & included contact details (you are advised to use your college email address as a relatively secure way in which to be contacted).
- You should ensure that the device locks if left inactive for a period of time & that entry of the password is required for it to unlock.
- You take all steps to protect your device from theft or damage.
- You have insured your device (& that use at college is covered).

☑ Charge your device before coming into college so that it can be used immediately.

☑ You should also ensure that all use of your device complies with the guidance on e-safety, copyright, data protection & handling of sensitive information referred to in other sections of this Acceptable Use Policy.

☑ To assist with protecting data, you should keep personal data & communications separate from college data. This can be achieved in different ways dependent on your device, but it is likely that using the College's RemoteNet for college business is the easiest & most reliable to implement. Note that certain college data, such as sensitive information, should never be stored on your own device.

☑ Scan any transferrable media that you may be given by someone else for viruses, malware or other malicious software.

☑ If your equipment fails in use during a lesson, you should let staff know who may be able to provide you with a college-owned device.

☑ Check your device & delete any sensitive or commercial emails once you have finished with them; delete copies of attachments to emails such as spreadsheets & data as soon as you have finished with them; limit the number of emails & other information that you sync to your device.

☑ When you need to save files, make sure you are in AcademicNet (the College's cloud offer).

☑ Use your device when on college premises in a manner that accords with both the spirit & letter of the Acceptable Use Policy.

Things not to do

☒ Do not bring your device into college if:-

- You have any concern about its electrical or other safety.
- You have any concern about how to keep it secure.

☒ Do not share any resources accessed at college with people or organisations outside of Wiltshire College without first seeking permission.

☒ Do not loan your device to someone else.

15. Enforcement

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

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

16. Acceptance

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

Students

Acceptance is electronic as part of your account activation & 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.

APPENDIX A

EMAIL AND INTERNET ADDITIONAL GUIDANCE

The use of external email and access to the Internet provides valuable opportunities for the College because they facilitate the gathering of information and support communication with others. However, Internet and email access also opens up the College to risks and responsibilities. It is therefore essential that users read these guidelines and make themselves aware of their responsibilities when using email and the Internet.

General Points

1. Use of email and the Internet is designed for work or course related purposes.

2. To comply with its legal responsibilities, the College monitors any and all aspects of its telephone and computer system that are made available to you and may intercept and/or record any communications made by users, including telephone, email or Internet communications. To ensure compliance with this guidance or for any other purpose authorised under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 users are hereby required to expressly consent to the College doing so. Consent occurs when a student activates their network account and when a staff member signs their induction checklist.

3. Computers and email accounts are the property of the College and are designed to assist in the performance of your work. This and inherent limitations of the technology dictate that you should have no expectation of privacy in any email sent or received, whether it is of a business or personal nature. Normally email will only be accessed by the College where it is believed abuse or inappropriate use is taking place.

4. It would be inappropriate use of email and the Internet to access, download or transmit any material, which is illegal or might reasonably be considered to be obscene, abusive, sexist, racist or defamatory. You should be aware that such material might also be contained in jokes sent by email. Such misuse of electronic systems will be misconduct and will, in certain circumstances, be treated by the College as gross misconduct. The College reserves the right to use the content of any email in any disciplinary process.

5. The College network is connected to the Internet via the Joint Academic Network (JANET). All use of the Internet and external email is subject to the JANET Acceptable Use Policy, which can be viewed at http://www.ja.net/documents/publications/policy/aup.pdf.

Use of email

6. Emails should be drafted with care. Due to the informal nature of email, it is easy to forget that it is permanent form of written communication and that material can be recovered even when it is deleted from your computer.

7. Users should not make derogatory remarks in emails about any individual, group or organisation. You remain personally liable for all of your email content, and should note that any written derogatory remark may constitute libel.

8. You must not create email congestion by sending trivial messages or unnecessarily copying emails. Users should regularly delete unnecessary emails to prevent over-burdening the college mail system.

9. Emails are stored for a limited time within the system (currently 13 months for staff, 30 days for students). You should make electronic copies outside of the email system of any messages which you need to retain for permanent record keeping purposes.

10. You may want to obtain email confirmation of receipt of important messages. You should be aware that this is not always possible and may depend on the external system receiving your message. If in doubt, telephone to confirm receipt of important messages.

11. Reasonable private use of email is permitted but should not interfere with your work. The contents of personal emails must comply with the restrictions set out in these guidelines. Excessive private use of the email system during working hours may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct.

12. By sending emails on the College's system, you are consenting to the processing of any personal data contained in that email and are explicitly consenting to the processing of any sensitive personal data contained in that email. If you do not wish the College to process such data you should communicate it by other means.

13. Emails sent outside the College have the College's standard email disclaimer notice added to them. You may add your own signature and text but you must not undermine or invalidate the College disclaimer in any way.

Use of the Internet

14. Reasonable private use of the Internet is permitted but should be kept to a minimum and should not interfere with your work. Excessive private access to the Internet during working hours may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct.

15. The sites accessed by you must comply with the restrictions set out in these guidelines. Accessing inappropriate sites may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct.

Copyright, downloading and attachments

16. Copyright applies to all text, pictures, video and sound, including those sent by email or on the Internet. Files containing such copyright protected material may be downloaded, but not forwarded or transmitted to third parties without the permission of the author of the material or an acknowledgement of the original source of the material, as appropriate.

17. Copyrighted software must never be downloaded without permission.

18. To minimise the risk of virus infection, users should not open any attachment unless they are from a known user and the attachment was expected or agreed by other means.

19. Users must never engage in political discussions through outside newsgroups using the College's computer system.

General computer usage

20. You are responsible for safeguarding your password for the system. For reasons of security, your individual password should not be printed, stored on-line or given to others. Password rights given to users should not give rise to an expectation of privacy.

21. Your ability to connect to other computer systems through the network does not imply a right to connect to those systems or to make use of those systems unless authorised to do so. You should not alter or copy a file belonging to another user without first obtaining permission from the creator of the file.

ICT Department

The ICT Department is here to assist you. If you require any information or help about the use of your computer or the College network, you should contact the ICT Help Desk on extension 6310 or email ITSUPPORT@wiltshire.ac.uk.

APPENDIX B

GLOSSARY & DEFINITIONS

BYOD	'**B**ring **Y**our **O**wn **D**evice' – when a person uses computing or communications equipment they own when connecting to College systems
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	Pronounced as **Control Alt Delete**, this abbreviation represents pressing all three of the CTRL, ALT & DELETE keys simultaneously. Using CTRL + ALT + DEL when you are logged in will display a menu on the screen. Options include:- • 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	**I**nformation & **C**ommunications **T**echnology – such as computers, the Internet, mobile communications, e-mail.
LT	**L**earning **T**echnology – the use of computers & communications technology for learning & teaching.
MIS	**M**anagement **I**nformation **S**ystems – used here to cover ICT, LT & in its more specific sense of management information systems, including information security.
Plagiarism	Proper academic practice means that you must only use other people's work (e.g. a quotation from a book) legally & in a way that clearly demonstrates that it is not your own work. Passing off other's work as your own or accidentally including something you have no right to have in your work are both examples of plagiarism.
Sensitive	The meaning of sensitive in this context is provided by the Data Protection Act, 1998, Part 1, Preliminary, item 2: "Sensitive personal data In this Act "sensitive personal data" means personal data consisting of information as to— (a) the racial or ethnic origin of the data subject, (b) his political opinions, (c) his religious beliefs or other beliefs of a similar nature, (d) whether he is a member of a trade union (within the meaning of the [1992 c. 52.] Trade Union & Labour Relations (Consolidation) Act 1992), (e) his physical or mental health or condition,

	(f) his sexual life, (g) the commission or alleged commission by him of any offence, or (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.”
Software	Any program that can be installed on your computer. Examples include:- • 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:- • Students • Employees • Temporary staff • Voluntary staff • Employees of partner organisations • Contractors & subcontractors • Agents • Work experience placements
You	You are defined as a user of Wiltshire College information systems

Wiltshire College

Information Systems Acceptable Use Policy

Agreed	August 2016
To be reviewed	August 2017