Wiltshire College & University Centre

Information Systems Acceptable Use Policy (Staff)

Contents

1. Introduction

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

2. Purpose of this policy

The purpose of this policy is to:

- Promote the professional, ethical, lawful & productive use of Wiltshire College & University Centre information systems
- Define & prohibit unacceptable use of Wiltshire College & University Centre information systems
- Educate users about their Information Security responsibilities
- Describe where, when & why monitoring may take place
- Outline related disciplinary procedures

3. Roles and responsibilities

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

4. Information Security within Wiltshire College & University Centre

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 & University Centre has implemented an 'Information Security Management System' to manage & continually improve Information Security over time, which is maintained by ICT Services.

5. 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 & University Centre information systems are provided to support college business.
- Use of any Wiltshire College & University Centre information system for personal reasons (including e-mail & the web) is only permitted in accordance with the guidance in this policy.
- Wiltshire College & University Centre monitors many aspects of its information systems 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 & University Centre information systems.
- All emails & other messages posted on college systems are covered by Wiltshire College & University Centre'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 conflicts with this policy, advice should be sought from a line manager or the College's Head of ICT.
- 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 may 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 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 & University Centre.
- Anything that will potentially harm your employment prospects.
- Anything that may lead to the display of extremist materials /views

6. Handling Personal and Sensitive Data

Things to know

- In the course of your work as a member of staff, you will come across personal and sensitive information. This could include:-
  - Personal data such as student work, email addresses, names and addresses
  - Sensitive data such as racial or ethnic origin, political opinions, religious beliefs, sexual preferences
  - Wiltshire College & University Centre's or third parties' Intellectual Property (such as product designs or software source code)
  - Confidential financial information (such as salary or financial planning data)
- Personal Data must be protected against disclosure to unauthorised parties.
- It is your responsibility to handle this information appropriately & in accordance with Wiltshire College & University Centre procedures.

Things to do

- When creating data, 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 personal data only to authorised parties using approved methods, after ensuring data protection sharing agreements are in place.
- Encryption is required when sending personal data, use only tools & guidance provided by Wiltshire College & University Centre 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 data with another party without a data sharing agreement in place.
- Do not remove/delete personal data without your manager's approval.
- Do not send personal data via the internet without your manager'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 unapproved instant messaging (Office 365 services are approved – any other system or service should be approved by the Data Protection Officer prior to use)
  - Using file transfer or file sharing web sites (such as Drop Box/Google Drive)
  - Using unapproved cloud storage or cloud-based systems e.g., DropBox/Google Drive/ShareFile etc (College Office365/SharePoint is approved – any other system or service should be approved by the Data Protection Officer prior to use)
- Do not copy personal data to any mobile device or removable media without your manager's approval. Common examples of removable media include:-
  - USB sticks, memory cards and external hard drives
  - CDs, DVDs
  - Electronic devices with data storage capacity (including phones, cameras)

7. College Equipment

Things to know

- College equipment is the property of Wiltshire College & University Centre & has been prepared by ICT Services for use on the Wiltshire College & University Centre network. Data saved to local (C:\) drives will not be backed up, & may be lost if the computer

breaks, gets stolen or is replaced. It is your responsibility to ensure the OneDrive sync client has successfully copied work to Office 365.

- Wiltshire College & University Centre 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

- Lock or log out of your workstation when you are away from it.
- Save data to Office 365 / Teams.
- Ensure that files received from anywhere outside the organisation are malware-checked before you open them. This process is 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 malware, 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 personal device you connect to the college system is approved for college use before using it. 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
- Do not disable or uninstall any of the software that is installed on your computer

8. 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
  - Smartphones
  - 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 (including Office 365 services) 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 access College systems and data (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
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; save on to OneDrive/Teams instead.
- 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.
- Never respond to a message that you were not expecting, e.g., Royal Mail delivery.
- Never supply banking or payment details in response to any message. This is a well-known method of smishing and fraud. Your bank will never request security details by message.

9. Your Identity / Password

Things to know

- Staff are issued a network login and an ID Badge which gives access to printing.
- Your Login, Password and ID Badge will control access to College resources.
- You can change your password at any time, not just when the system prompts you.

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 Reception, Estates, The 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 10 characters and all of the following: -
    - upper case characters
    - lower case characters
    - numbers
    - special characters/symbols
- Change your password if you suspect that someone else may know it.

Things not to do

- Do not write passwords down
- Do not disclose your password to anyone. Even ICT Services staff, they do not need to know it and can change it if required.
- Do not give your network login or ID Badge to anyone else.
- Do not use anyone else's login, ID Badge or password.

10. E-mail

Things to know

- Wiltshire College & University Centre e-mail systems are provided for college use.
- Wiltshire College & University Centre monitors all e-mail to ensure compliance with policy.
- 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.
- Make sure that your message is concise, relevant only sent to the people who need to read it.
- When sending emails to multiple people containing data use BCC not CC, to ensure recipients do not see others' personal data. Use the telephone or face to face conversation instead of e-mail where this is possible & appropriate.
- Use the 'Scheduling Assistant', 'Out of Office Assistant' and 'free'/'busy' status to plan meetings and let people know when you are free.
- 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 use e-mail to rebuke, criticise or complain about somebody without careful consideration. You may say something that you regret, the record will be permanent and could be disclosed in a subject access request.
- 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
    - Malware or phishing 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 is personal or sensitive without their express consent. Using initials doesn't stop an individual from being identifiable when used in conjunction with other information.

11. Web Browsing

Things to know

- Access to the web is provided for college use. Reasonable personal use is permitted and is defined later in this policy.
- Wiltshire College & University Centre monitors and records all web browsing to ensure compliance with policy.
- 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 malware infection on your computer. 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

12. Printing

Things to know

- Printers are provided for college use only.

Things to do

- Be selective about what you print. Print only what you need. The College is committed to improving environmental sustainability, and reducing printing makes an important contribution to this goal.
- Print double-sided where possible to save paper
- Observe published print procedures and guidance.
- Keep the area around printers tidy

Things not to do

- Do not print anything that is likely to infringe copyright

13. Personal Use

Wiltshire College & University Centre recognises that personal access to the web at college helps staff to maintain a positive college work life balance. Limited and 'reasonable' personal use of the web is permitted. Reasonable use is defined below. Personal use of all other college systems is prohibited.

Web access for personal use is provided at considerable risk & cost to the organisation. Wiltshire College & University Centre expects that 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, for example, to spend more time than you intend to on 'addictive' sites like auctions, gaming, social networking and blogging.

All college systems are monitored to ensure compliance with college policies. Staff who 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 & University Centre 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 web) for personal reasons, either for yourself or on behalf of others. This would breach the Data Protection Act 2018.
- Activities for personal financial gain or for private business purposes.

14. 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 & University Centre governors and staff being personally liable to criminal prosecution.
- Wiltshire College & University Centre being sued for damages in a civil court.

Things to do

- Comply with software licences, copyright and 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 2018. Your 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.

15. Monitoring

Wiltshire College & University Centre 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 & University Centre 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 & University Centre
- Protect Wiltshire College & University Centre from legal liability

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

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

- The Head of Human Resources
- The appropriate line or senior manager
- The Police

16. Using Your Own Equipment (BYOD) either remotely or on the College Network

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 or connecting remotely.
- In using your own device to access college data, 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).
- 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:
    - 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.
    - Up to date Anti malware software must be installed on your device before connecting it to the College network or accessing college data.
    - Updates related to the security of software & operating systems on your device are kept up to date and installed with 14 days of their release.
    - 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.
    - The device has its firewall turned on.
    - You take all steps to protect your device from theft or damage.
- 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. 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 malware.

- Do not save any personal or sensitive data on the device. Choose to work exclusively using web versions of products to ensure local copies of data do not exist on the personal device. When you need to save files make sure you are using Office 365 on the web.
- 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 & University Centre without first seeking permission.
- Do not loan your device to someone else.

17. Enforcement

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

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

18. Acceptance

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

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 Staff

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.

19. Equality Statement

It is intended that this policy is 'fair to all'. Where any part could potentially lead to unequal outcomes, the procedure then justifies why this is a proportionate means of achieving a legitimate aim.

20. Data Retention Statement

Wiltshire College & University Centre is committed to ensuring the data it collects, and holds is in line with the ICO's guidance and meets Data Protection law. Where appropriate a Data Protection Impact Assessment will be undertaken as and when policies are updated to ensure risks to the individual and college are considered and managed.

21. Policy Review and Ownership

This document is owned and managed by ICT Services. The policy will be reviewed and amended as required, and at least every two years by the Head of ICT Services or appropriate substitute, and subject to approval by the College's Senior Leadership Team.

22. Amendments Log

Version	Date of Issue	Amendment summary	Author(s)
V1.0	29/04/2019	Approved by SMT	Phil Lewis
V1.1	02/03/2021	Reviewed – no change – review date extended.	Phil Lewis
V1.2	29/09/2021	Addition of section 17. No other changes	Phil Lewis
V1.3	17/08/2022	Section 6. Sensitive information now personal information and added data sharing agreements	
V1.3	17/08/2022	Section 7. Your computer now college equipment. Added cloud storage statement	
V1.3	17/08/2022	Section 9. Updated password management	
V1.3	17/08/2022	Section 16. Updated using own equipment and added home device management	
V1.3	17/08/2022	Removed Section 17. Connecting to network remotely.	

APPENDIX A

EMAIL AND INTERNET ADDITIONAL GUIDANCE

The use of 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 may monitor any aspects of systems that are made available to you. 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 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. You should have no expectation of privacy in any email sent or received, whether it is of a business or personal nature. Normally accounts 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 or browsing history 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 https://community.jisc.ac.uk/library/acceptable-use-policy

Use of email and Teams

6. Messages should be drafted with care. Due to the informal nature of email and instant messages, it is easy to forget that it is a 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 messages about any individual, group or organisation. You remain personally liable for all of your message

content and should note that any written derogatory remark may constitute libel.

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

9. Emails are stored for a limited time within the system. 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. 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.

12. 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 malware infection, users should not open any attachment unless they are from a known user and the attachment was expected or agreed by other means.

General computer usage

19. 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.

20. 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.

IT Services

IT Services 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 IT 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.
Office 365	Suite of web-based applications that are accessible via the College web site. These include Mail, Calendar, OneDrive, SharePoint, OneNote, Sway, Teams, Planner, Yammer and more …
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, 2018: "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 or genetic or biometric data, (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.”
Smishing	Phishing via SMS messaging
Software	Any program that can be installed on your computer. Examples include:- • Microsoft Word • An Antimalware 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 & University Centre 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 & University Centre information systems