TITLE	REF	VERSION
IT Acceptable Use Procedures	IT005	4

Department	DATE	REVIEW DATE
Institutional Effectiveness	29 September 2024	29 September 2026

IT SERVICES ACCEPTABLE USE PROCEDURES

Contents

1. IT Services Acceptable Use Procedures

This procedure applies to:

- All employees, students and visitors that use equipment provided by Activate Learning
- All employees, students and visitors that use software provided by Activate Learning
- All employees, students and visitors that use accounts provided by Activate Learning
- All employees, students and visitors that access the physical network provided by Activate Learning
- All employees, students and visitors that connect to the network provided by Activate Learning
- All employees, students and visitors that connect to the network provided by Activate Learning from any remote location

Sections or clauses that are relevant to employees only are marked as such.

2. Your Computer

2.1. Things to know:

- “Your” computer is the property of Activate Learning and has been prepared by the IT Services team for use on the Activate Learning network.
- Data saved to local drives will not be backed up, and will be lost if your computer breaks, gets stolen or is replaced.
- Activate Learning may at any time and without prior notice Audit your computer to ensure compliance with this policy
- Require the return of your computer and any associated equipment

2.2. Things to do:

- Lock your workstation (CTRL+ALT+DEL) when you are away from it.
- Ensure that files received from anywhere outside of Activate Learning are virus checked before you open them. This includes files on CD’s/DVD’s, USB drives, smartphones, or any other media.
- If you suspect that you may have a virus, leave your computer on, unplug the network cable, and contact the IT Service Desk.
- Turn your PC and monitor off at night to save energy unless there is a valid specific reason to leave it on.

2.3. 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 the IT Service Desk. Things that you should never attempt to install (without prior agreement of the IT Services/Digital Education Services and AI teams) include but are not limited to:
    - Games
    - Music download software
    - Messaging software
    - Telephony software
- Utilities that claim to remove spyware or viruses
- News readers or peer to peer software

- AI chatbots, resources and tools
- Do not disable or uninstall any of the software that is installed on your computer
- Never plug in any found USB or other media into an Activate Learning device

3. Portable Devices

3.1. Things to know:

- You should read and understand this section even if you do not normally use a portable computer/device. You may need to do so at some point in the future.
- You are responsible for the care and safe storage of any computer equipment that has been issued to you.
- The term 'portable computer/device' covers any Activate Learning-owned mobile computing device including:
    - Laptop
    - Tablets
    - Smartphones

3.2. Things to do:

- Back up your work to the network at regular intervals
- Always consider the physical security of your portable computer/device:

In an unlocked office	Secured with a cable or kept in a locked drawer
In the car	Concealed from view. Ideally in a locked boot or glove compartment
At home	Take normal precautions to ensure the computer is always secure.
In a hotel	Concealed from view. Ideally locked in a suitcase
Travelling	Always keep the computer on your person and secure

3.3. Things not to do:

- 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 computer.
- Do not leave portable computers/devices in the car unless absolutely necessary.
- Never connect your computer/device to an unapproved network (such as coffee shop or a hotel access point) unless you have gained permission from the IT Service Desk.

4. Your Password

4.1. Things to know:

Password Policy:

- You cannot use the last 12 passwords
- You will be forced to change your password every 180 days
- Passwords must be 8 characters or more
- If you enter the wrong password 20 times you will be locked out for a period 10 minutes. (IT Services can override this timeout when resetting your password if you have forgotten it)
- 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, the IT Service Desk can help you with this. You do not need to share passwords.
- The access rights associated with your user account may be changed or revoked should your employment or programme of study change or be terminated.

4.2. Things to do:

- Set a password or phrase. Make it as secure as you can by using at least three 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.

4.3. Things not to do:

- Do not disclose your password to anyone. Even IT staff do not need to know it.
- Do not use anyone else's password.

5. Email and Instant Messaging

5.1. Things to know:

- Activate Learning systems are provided for business use. Reasonable personal use is permitted and is defined later in this procedure.
- Activate Learning monitors all e-mail and instant messaging to ensure compliance with policy.
- Email is not a secure method of communication. Once a message is sent you have no further control over who reads it.
- For employees, email is admissible in court and carries the same weight as a letter on Activate Learning headed paper.

5.2. Things to do:

- For employees, use the same care when drafting an email message as you would when writing a letter on Activate Learning headed paper.
  For all users:
- Make sure that your message is concise, relevant, and sent only to the people that need to read it.
- Clear out old and unwanted messages from your mailbox and empty your deleted items folder.
- Ensure any sensitive data has been encrypted and locked with a password before emailing it to any third parties.

5.3. Things not to do:

- For employees, do not send all staff emails about anything that is not work related. For example, charity requests or lost notices etc.
- For employees, never reply all to an all-staff email

- For employees, do not circulate non-work-related material. This includes but is not limited to:
    - Jokes and chain letters, music, pictures, videos or software
    - For all Users:
- Never reply all to a large distribution group email.
- Never open an attachment that you were not expecting. Even if you know the sender.
- Never supply banking or payment details in response to an email message. This is a well-known method of fraud. Your bank will never request security details by email.
- Do not use email to send sensitive or confidential information unless included in an attachment that is password protected.
- Do not send or forward anything that:
    - Is covered by a copyright or that others may find offensive
    - May be defamatory (about an individual or organisation)
- Do not disclose any information about a person that you would object to being disclosed about yourself
- Never use email to rebuke, criticise or complain about somebody. You may say something that you regret, and the record will be permanent.

6. Web Access

6.1. **Things to know:**

- Web access is provided for business use. Reasonable personal use is permitted and is defined later in this policy.
- Activate Learning monitors and records all web / application access to ensure compliance with this policy. This includes laptops, tablets and mobile phones on the guest wireless network.
- Access to certain web sites may be blocked in order to protect you and Activate Learning. 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.

6.2. Things to do:

- Inform the IT Service Desk if access to a legitimate and business-related web site is blocked.
- Inform the IT Service Desk 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.

6.3. 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 use the web for listening to radio or watching video unless for legitimate curriculum activity.
- 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 music downloads or films
- Free software and serial numbers
- Adult material
- Pirate sites for download illegal software and films
- Radicalisation and Extremism

7. Printing

7.1. Things to know:

- Colour printers cost much more per page than black and white ones. Even if there is no colour on the page.
- Printers are provided for business use only.
- All printing is monitored, and credit limits are set for learners and staff.
- Printing retries timeouts and page count limits apply.

7.2. 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.
- Use a photocopier when producing many copies and make use of reprography where possible.
- Keep the area around MFD copiers tidy.

7.3. 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:
    - Do you have enough credit?
    - Has the job been denied due to resending it to quick or because of a high page count?
    - Is the print job still listed in the queue?
    - Is the copier switched on?
    - Is the copier in an error state because:
        - There is paper jam
        - It is out of paper
        - It is out of toner or ink
- Report any errors to the IT Service Desk and do not attempt to fix them yourself.
- Do not shake toners cartridges.
- Do not allow your ID card to be used for printing other than your own.

8. Use of Resources

8.1. Things to know:

- Implementing the small changes described on this page can make a big difference to the organisation’s costs, and to the environment.
- Phone chargers and AC adapters consume a small amount of power even when nothing is connected to them.

8.2. Things to do:

- Shut your computer down at the end of your working day rather than just logging off. The energy saved over a year is enough to boil 60 tonnes of water.
- Turn off your monitor before you leave rather than leaving it in standby (1.5 tonnes).
- Unplug or switch off phone, tablet, or laptop chargers when they are not in use.
- Preserve laptop battery power by shutting it down and not just closing the lid.
- For employees, turn off Interactive Whiteboards and speakers at the end of the lesson.

8.3. Things not to do:

- Do not turn off computer equipment on behalf of someone else. There may be a good reason why it has been left on.
- Do not turn off Printers.

9. Reasonable personal use of Activate Learning systems is that which:

- Is lawful and ethical.
- Is in accordance with this policy.
- Does not adversely affect your productivity.
- Does not make unreasonable use of limited Activate Learning resources.
- For employees, takes place during breaks or outside of your working hours.

10. Unreasonable personal use of Activate Learning systems includes but is not limited to:

- Contravention of this policy in any way.
- 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 professional working environment.
    - Activities for personal financial gain.
    - Use for business other than that of Activate Learning.

11. Legal Responsibilities

11.1. 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.
    - Activate Learning management being personally liable to criminal prosecution.
    - Activate Learning being sued for damages in a civil court.

11.2. 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 work, you must do this in accordance with the Data Protection Act 1998 and the General Data Protection Regulations 2018.
- Report any data breaches or loss of equipment with personal data on them to IT Services Team within 24 hours. Activate Learning's Data Protection Officer and the ICO will be notified within the next 48 hours. Failure to report a breach will result in a significant fine for Activate Learning.
- Ensure any personal and Activate Learning data is stored on encrypted devices or encrypted USB drives.

11.3. Things not to do:

- Do not borrow or copy Activate Learning software for use at home or elsewhere, unless properly authorised and the appropriate agreement has been signed.
- Do not write or say anything defamatory or potentially libellous about another individual or company.
- Do not store personal or Activate Learning data onto a memory stick that is not encrypted.

- Do not keep any information about a security breech to yourself. If in doubt, report it.
- Do not store Activate Learning data on your own personal devices.

12. Online Safety and PREVENT

12.1. Activate Learning takes all reasonable actions to limit exposure to risks while using college-owned devices and IT services. This includes the use of appropriate filtering and monitoring systems, which are regularly reviewed for effectiveness in line with the Department for Educations' Filtering and Monitoring Standards for Schools and Colleges

12.2. The Government's PREVENT strategy focuses on identifying and supporting vulnerable individuals who may be at risk of being exploited by radicalisers, especially online. It is crucial to be vigilant and proactive in preventing exposure to radicalizing influences.

12.3. **Important Actions:**

- Report Concerns: If you have any concerns related to Safeguarding or PREVENT, immediately report them to Activate Learning's Safeguarding team: safeguarding@activatelearning.ac.uk
- This includes adhering to the Government's 'Prevent, Pursue', 'Protect', and 'Prepare' principles for the UK Strategy for Countering Terrorism 2023 .

12.4. **What to Avoid:**

- Avoid Extremist Content: Do not access websites or platforms that promote extremism, including content that opposes fundamental British values such as democracy, the rule of law, individual liberty, and mutual respect and tolerance for different faiths and beliefs.
- Do Not Share Extremist Material: Refrain from sharing any extremist websites or information through electronic communication channels.
- By following these guidelines, we can ensure a safer online environment and contribute to the overall safety and well-being of our learning community.

13. Monitoring and Tracking

13.1. Activate Learning reserves the right to monitor any of its systems at any time. This includes the use of the guest wireless network.

13.2. You should have no expectation of privacy when using Activate Learning systems, whether for business or personal use.

13.3. 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 Activate Learning
- Protect Activate Learning from legal liability

13.4. Monitoring reports will be viewed and analysed only by the designated lead in IT Services and his/her nominated representatives. In the event of the IT Services representative being implicated, the data will be referred to the Group Director of Institutional Effectiveness, and then to the Chief Operating Officer.

13.5. If a member of staff identifies possible misuse of Activate Learning systems, they should inform, as soon as possible, the Group Director of Institutional Effectiveness, who will instigate an appropriate investigation. During these investigations, all related matters will be treated in the strictest confidence.

13.6. On instruction of the Group Director of Institutional Effectiveness, the data may be passed as necessary to any of the following:

- The appropriate line manager
- The Chief People Officer
- The Police (by agreement with a member of the Group Executive Team).

a. Activate Learning uses GPS tracking for theft and crime prevention on all its assets these include but are not limited to PC’s Laptops, Tablets and Mobile Phones.

14. Removable Media

14.1. This procedure and associated policy apply to all employees, students, contractors, and third-party vendors who have access to company-owned devices or company data.

14.2. Removable media devices, including but not limited to USB drives, CDs, DVDs, and external hard drives, are not permitted on company-owned devices or network systems without prior approval from IT Services. The use of this type of media is blocked by a network level restriction policy.

14.3. Employees must not copy, transfer, or store sensitive company data on removable media devices, unless there is a specific Examination or Media requirement, and it has been authorised and encrypted by IT Services.

14.4. Employees must report any lost or stolen removable media devices to IT Services immediately. In case of loss or theft of a removable media device, IT Services will initiate a data breach investigation to assess the potential impact on the company's data.

15. Remote Working for Employees

15.1. The college-provided IT equipment has a range of security measures enabled to make home working safer. Do not use personal devices for downloading, storing, accessing, or transmitting commercially sensitive information.

15.2. The College IT Acceptable Use Policy (HYPERLINK) should be adhered to when remote working; this includes locking a device when not in use, not disclosing any passwords, multi-factor authentication PINs or encryption keys. It is the responsibility of the remote worker to safeguard and protect any College information that they hold.

15.3. Activate Learning SharePoint Apps and Secure Remote Gateway / VPN services provide a secure channel with multi-factor authentication for data transfer over insecure networks and should be used by remote workers when interacting with college resources. This includes but is not limited to use with desktops, laptops, tablets, and smartphones.

15.4. Digital information must only be downloaded or uploaded over a secure connection. Wi-Fi networks offered at airports, hotels, coffee shops and on public transport are generally insecure and extra measures must be taken to safeguard against information loss.

15.5. IT Equipment is provided for work purposes and must be used in accordance with the Acceptable Use Policy. Reasonable care must be taken of College owned IT equipment including steps to minimize the risk of theft or damage to equipment that is kept offsite for remote working.

15.6. Equipment in transit or left in a stationary vehicle must be locked securely out of sight. Employees will be responsible for the cost of equipment which is damaged or lost due to their own negligence. It is advisable, for this reason, that employees clarify whether their personal insurance will cover them for damage or loss due to negligence.

15.7. Employees must return to the College, all equipment at the end of any remote working arrangements to the IT Services Department.

16. References

Other documents or useful information related to this procedure includes:

b. IT Acceptable Use Policy
c. Positive Behaviour Management Policy
d. Artificial Intelligence Usage Policy
e. Safeguarding and Child Protection Policy
f. Online Safety Policy

If this document is required in an alternative format, please contact:
complianceteam@activatelearning.ac.uk