ICT Acceptable Use Policy

Version:	v1.0
Policy Type:	People – Good Practice
Approval date:	18 October 2023
Approved by:	Trust Board
Next review:	Autumn 2026

Together we Exceed

Contents

1. Statement of Intent

1.1 Exceed Academies Trust believes that ICT plays an important part in both teaching and learning over a range of subjects. The Trust is committed to ensuring that both staff and pupils have access to the necessary devices, facilities and support to allow them to carry out their work.

1.2 The Trust has a sensible and practical approach that acknowledges the use of devices, and this policy is intended to ensure that:

1. Members of staff are responsible users and remain safe while using the internet.
2. ICT systems and users are protected from accidental or deliberate misuse which could put the security of the systems and/or users at risk.
3. Members of staff are protected from potential risks in their everyday use of electronic devices.

1.3 Personal use of ICT equipment and personal devices is NOT permitted within the Trust. Access to school / Trust Microsoft Office 365 systems is permitted on personal devices if required by use of the relevant Microsoft application or internet browser.

2. Legal Framework

2.1 This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

1. The General Data Protection Regulation (GDPR)
2. The Data Protection Act 2018
3. The Computer Misuse Act 1990
4. The Communications Act 2003
5. The Freedom of Information Act 2000
6. The Human Rights Act 1998
7. Voyeurism (Offences) Act 2019

3. Roles and Responsibilities

3.1 The Headteacher is responsible for:

1. The day-to-day implementation and management of the policy.
2. The overall allocation and provision of resources.

3.2 The ICT Technical Lead / External Support team are responsible for:

1. Monitoring Internet systems for inappropriate use and reporting such findings to the relevant headteacher or Trust representative.
2. Monitoring server and device logs on the network and to report any logged inappropriate use to the headteacher or Trust representative.
3. Remotely viewing or interacting with any of the computers on the network. This may be done randomly to implement this policy and to assist in any difficulties.
4. Ensuring routine security checks are carried out on all devices and that security software is in place and being updated.
5. Ensuring that staff are made aware of the potential risks, whilst taking appropriate steps to ensure personal information is not seen during security checks.
6. Accessing files and data to solve problems for a user, with their authorisation.
7. Adjusting access rights and security privileges in the interest of the protection of the

School's / Trust data, information, network and computers.

8. Disabling user accounts of staff that do not follow the policy, at the request of the headteacher or Trust representative.
9. Assisting the headteacher or Trust representative in all matters requiring reconfiguration of security and or access rights and in relation to this policy.
10. Assisting staff with authorised use of the ICT facilities and devices, as and when required.
11. Immediately reporting any breach of personal information or information leakage to the DPO.
12. Ensuring that all School and Trust owned devices are secured and encrypted in line with the Trusts Data Protection Policy.

3.3 The DPO is responsible for:

1. Auditing, at random, school-owned devices to ensure they meet the security requirements detailed in this document, to protect sensitive data in cases of loss or theft.
2. Ensuring all staff are aware of, and comply with, the data protection principles outlined in the Trust's Data Protection Policy.

3.4 Staff members are responsible for:

1. Requesting permission from the Headteacher or ICT Technical Lead, subject to their approval, before using school-owned devices for personal reasons during or outside of school hours.
2. Requesting permission to loan school equipment and devices from the Headteacher or member of SLT.
3. Reporting misuse of ICT facilities or devices, by staff or pupils, to the Headteacher or Trust representative.
4. Reading this and other related policies.
5. Agreeing to this policy. Agreement to this policy by all staff is taken by the acceptance of the user agreement message displayed prior to logon. By clicking 'okay'; all users accept the terms within this and other related policies.

4. Classifications

4.1 School / Trust owned ICT facilities include, but are not limited to, the following:

1. Computers/laptops and software
2. Monitors
3. Keyboards
4. Mouses
5. Scanners
6. Cameras
7. Camcorders
8. Other devices including furnishings and fittings used with them
9. Mail systems (internal and external)
10. Internet and intranet (email, web access and video conferencing)
11. Telephones (fixed and mobile)
12. Tablets and other portable devices
13. Pagers
14. Fax equipment
15. Computers
16. Photocopying, printing and reproduction equipment

17. Recording/playback equipment
18. Documents and publications (any type of format)

5. Acceptable Use

5.1 The Trust monitors the use of all ICT facilities and electronic devices. Members of staff will only use school-owned devices for work duties and educational purposes. The duties for which use is permitted include, but are not limited to, the following:

a. Preparing work for lessons, activities, meetings, reviews, etc.
b. Researching any school-related task
c. Any school encouraged tuition or educational use
d. Collating or processing information for school business
e. Communication and collaborations which are deemed necessary to undertake your role

5.2 Inappropriate use of school-owned and personal devices could result in a breach of the Trust's Data Protection Policy.

5.3 Inappropriate use of school-owned and personal devices could result in a breach of legislation, including the GDPR and Data Protection Act 2018.

5.4 Any member of staff found to have breached the Trust Data Protection Policy or relevant legislation may face disciplinary action.

5.5 This policy applies to any computer or other device connected or not connected to the School / Trusts network.

5.6 Staff should always be an example of good practice to pupils, serving as a positive role model in the use of ICT and related equipment.

5.7 School / Trust owned electronic devices must not be used to access any material which is illegal, inappropriate, or may cause harm or distress to others.

5.8 Any illegal, inappropriate or harmful activity must be immediately reported to the ICT Technical Lead who will discuss the appropriate action with the headteacher.

5.9 Members of staff must not open email attachments from unknown sources.

5.10 Members of staff must not use programmes or software which may allow them to bypass the filtering or security systems of the School or Trust.

5.11 Members of staff will not upload or download large capacity files (over 500MB) without permission from the ICT department.

5.12 All data is stored appropriately and securely in accordance with the school's Data Protection Policy.

5.13 Members of staff only use School / Trust owned electronic devices to take pictures or videos of people who have given their consent.

5.14 School / Trust owned electronic devices should not be used to access personal social media, email or cloud based data storage accounts.

5.15 Personal electronic devices must not be used to communicate with pupils or parents, including via social media.

5.16 Staff representing the school or Trust online will express neutral opinions and will not disclose any confidential information or comments regarding the School / Trust, or any information that

may affect its reputability.

5.17 Staff will ensure the necessary privacy settings are applied to any social networking sites.

5.18 Images or videos of pupils, staff or parents will only be published online for the activities which consent has been sought.

5.19 Staff will not give their home address, phone number, social networking details or email addresses to pupils or parents – contact with parents will be done through authorised school contact channels.

5.19 Copyrighted material is not to be downloaded or distributed.

5.21 School / Trust owned devices can be taken home for work purposes only, once approval has been sought from the headteacher and the appropriate documentation has been completed.

5.22 Remote access to the School / Trust network can be provided upon request to staff using these devices at home.

5.23 School /Trust equipment that is used outside the premises, e.g. laptops, will be returned when the employee leaves employment, or if requested to do so by the headteacher, Trust representative or ICT Technical Lead.

5.24 While there is scope for staff to utilise School / Trust equipment for personal reasons, this will not be done during working hours unless approved by the headteacher or in the case of a personal emergency.

5.25 Private business must not be mixed with official duties, e.g. work email addresses should be reserved strictly for work-based contacts only.

5.26 Where permission has been given to use the School / Trust equipment for personal reasons, this use should take place during the employee's own time, e.g. during lunchtime or after school.

5.27 Abuse of ICT facilities or devices could result in privileges being removed and or disciplinary action.

5.28 Failure to adhere to the rules described in this policy may result in disciplinary action, in line with the Disciplinary Policy and Procedure.

6. Emails and the Internet

6.1 The email system and internet connection are available for communication and use on matters directly concerned with School / Trust business.

6.2 Abusive messages will not be tolerated – any instance of abuse may result in disciplinary action.

6.3 If any email contains confidential information, the user must ensure that the necessary steps are taken to protect confidentiality through message encryption.

6.4 The ICT department can provide assistance on how to encrypt email messages for the transfer of sensitive and or personal data through Office 365 or other alternative encryption systems.

6.5 The School / Trust email system and accounts must never be registered or subscribed to spam or other non-work-related updates, advertisements or other personal communications. Email addresses must not be shared without confirming that they will not be subjected to SPAM or sold on to marketing companies.

6.6 All emails being sent to external recipients will contain the School / Trust standard confidentiality notice. This notice is normally configured as an additional signature by the ICT department and must not be removed.

6.7 Staff linking work office 365 accounts to personal mobile devices – This must be configured using the relevant Microsoft application only i.e. Outlook. This is to ensure that access can be revoked in the event of loss or theft of the device.

6.8 The types of information sent through emails to a personal device will be limited to ensure the protection of personal data, e.g. pupils' details.

6.9 Contracts sent via email or the internet are as legally binding as those sent on paper. An exchange of emails can lead to a contract being formed between the sender, or the School / Trust, and the recipient. Staff must never commit the School or Trust to any obligations by email or the internet without ensuring that they have the authority to do so.

7. Portable Equipment

7.1 Data stored in user folders on School / Trust owned equipment is only synchronised with the school servers when connected to the network. Once synchronised this data is backed up through the School / Trusts backup routines.

7.2 Portable School and Trust owned electronic devices are not left unattended, are kept out of sight and are securely locked in a lockable cupboard in the staffroom or classroom when they are not in use.

7.3 Portable equipment is transported in its protective case, if supplied.

7.4 Where the School or Trust provides mobile technologies, such as phones, laptops and personal digital assistants, for off-site visits and trips, only these devices are used.

7.5 All portable devices such as phones and tablets must be secured with a minimum of four-digit pin code.

8. Removable Media

8.1 Only recommended removable media is used including, but not limited to, the following:

a. USB drives and other SSD media
b. DVDs
c. CDs
d. External hard drives

8.2 All removable media is securely stored in a lockable cupboard when not in use.

8.3 Personal and confidential information will not be stored on any removable media.

8.4 All removable media devices will be encrypted.

8.5 Removable media is disposed of securely by the ICT department.

9. Cloud-Based Storage

9.1 The Schools / Trust are aware that data held in remote and cloud-based storage is still required to be protected in line with the GDPR and DPA 2018.

9.2 Members of staff must ensure that cloud-based data is kept confidential and no data has the potential to be copied, removed or adapted.

9.3 Sensitive and personal cloud stored data should not be shared externally to the Trust.

10. Trust Issued Mobile Phones and eSims

10.1 Employees issued with a Trust mobile phone are responsible for their appropriate use and care.

10.2 Any loss, damage, or suspected security breach involving the mobile phone or eSIM must be reported to the IT department immediately.

10.3 Limited personal use of Trust mobile phones is permitted during non-working hours or breaks for emergencies only.

10.4 For Data Protection Purposes, Apple and Google Play Store Accounts should be registered to your work email account.

10.5 Personal use should not interfere with work responsibilities or incur additional costs for the Trust.

10.6 Employees are responsible for any personal charges incurred on the Trusts mobile phone.

10.7 Trust mobile phones may contain sensitive information. Employees must ensure they inform the IT Department following the appropriate channels if the security and confidentiality of company data stored on the device becomes unsafe.

10.8 Mobile phones must be protected with a strong PIN or password and should not be left unattended.

10.9 If for any reason the Trust feels there has been a breach to the security of a device, or it has been lost or stolen, a decision will be made to remotely erase the phone. The trust holds no responsibility for the loss of any personal data in line with the Data Protection Policy.

10.10 Trust issued mobile phones and eSIMS are intended for business communication purposes only, including calls, emails, and text messages related to work.

10.11 Employees are advised to only use the Microsoft Outlook App for emails as this is more secure than the native mail app on phones.

10.12 Employees should use professional language and conduct themselves appropriately when communicating using Trust mobile phones.

10.13 Employees must comply with all applicable laws and regulations regarding the use of mobile phones, including but not limited to data protection and privacy laws.

10.14 Any use of Trust mobile phones or eSim for illegal or unethical activities is strictly prohibited.

10.15 Mobile phones provided by Exceed Academies Trust are Trust property and are monitored and managed by the IT department via Sophos Mobile Device Management.

10.16 Employees must not modify or tamper with the management software or settings of Trust issued mobile phones without authorisation.

10.17 Employees are encouraged to report any issues or concerns regarding the use of Trust

mobile phones to their supervisor or the IT department.

10.18 Any suspected security breaches or unauthorised use of Trust mobile phones must be reported immediately.

10.19 Upon termination of employment, employees must return Trust issued mobile phones to the IT department who will ensure that all company data is removed from the device before it is reassigned.

10.20 If any unapproved overseas costs are incurred, these will be charged back to the employee who incurred the costs.

11. Storing Data

11.1 Information and data on the School or Trusts networks and computers will be kept in an organised manner and should be placed in a location of an appropriate security level.

11.2 If a member of staff is unsure about the correct storage procedure, help will be sought from the ICT department.

11.3 Personal data in the form of documents, photos, videos etc shall not be stored on, or copied to and from the school's systems.

11.4 Under no circumstances will Data for which the copyright is not held be stored on school or Trust systems.

12. Unauthorised Use

12.1 Staff are not permitted, under any circumstances, to:

1. Use the ICT facilities for personal commercial or financial gain.
2. Physically damage ICT and communication facilities or school-owned devices. The school / Trust reserve the right to recharge employees for damage caused to devices.
3. Relocate, take off-site, or otherwise interfere with the ICT facilities without the authorisation of the ICT Technical Lead or headteacher.
4. Use or attempt to use someone else's user account. All users of the ICT facilities will be issued with a unique user account and password. The password must be changed at regular intervals. User account passwords must never be disclosed to, or by anyone.
5. Use the ICT facilities at any time to access, download, send, receive, view or display any of the following:
   a. Any material that is illegal or breaches copyright laws.
   b. Any message that could constitute bullying, harassment (including on the grounds of sex, race, religion/religious belief, sexual orientation or disability) or any negative comment about other persons or organisations
   c. Online gambling
   d. Remarks, which may adversely affect the reputation of any organisation or person, whether or not you know them to be true or false
   e. Any adult or sexually explicit content, including chat and online dating systems
6. Generate messages or documents that appear to originate from someone else, or otherwise impersonate someone else.
7. Install hardware or software without the consent of the ICT department.

8. Introduce any form of stand-alone software or removable hardware likely to cause malfunctioning of the ICT facilities or that will bypass, over-ride or overwrite the security parameters on the network or any of the School's / Trusts systems.
9. Use or attempt to use the School / Trusts ICT facilities to undertake any form of piracy, including the infringement of software licenses or other copyright provisions whether knowingly or not.
10. Purchase any ICT facilities or devices without the consent of the ICT Technical Lead and or headteacher. This is in addition to any purchasing procedures followed according to the Finance Policy.
11. Use or attempt to use the School / Trusts phone lines or mobile devices for internet or email access. This includes using or attempting to use any other form of hardware capable of telecommunication, regardless of ownership.
12. Use or attempt to use the School / Trusts phone lines or mobile devices for personal calls unless prior approval has been sought from the headteacher or Trust representative.
13. Use any chat-lines, bulletin boards or pay-to-view sites on the internet.
14. Use the internet for any auctioning activity or to purchase items unless given authority to do so by the headteacher or Trust representative. This is in addition to any purchasing procedures followed according to the Finance Policy.
15. Knowingly distribute or introduce a virus or harmful code onto the School / Trust network or computers. Doing so may result in disciplinary action, including summary dismissal.
16. Copy, download or distribute any material from the internet or email that may be illegal to do so. This can include computer software, music, text, and video clips. If it is not clear that you have permission to do so, or if the permission cannot be obtained, do not do so.
17. Use, or attempt to use, the communication facilities to call overseas without the authorisation of the headteacher or Trust representative.
18. To obtain and post on the internet, or send via e-mail, any confidential information about other employees, the school, the Trust, its learners, customers or suppliers.
19. Interfere with someone else's use of the ICT facilities.
20. Be wasteful of ICT resources, particularly printer ink, toner and paper.
21. Use the ICT facilities when it will interfere with your responsibilities to supervise pupils.
22. Share any information or data pertaining to other staff or pupils at the school with unauthorised parties. Data will only be shared for relevant processing purposes and will be suitably secured through encryption.
23. Operate equipment to record an image beneath a person's clothing with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks without their knowledge or consent (whether exposed or covered by underwear) – otherwise known as "upskirting".

12.2 Any unauthorised use of email or the internet is likely to result in disciplinary action, including summary dismissal, in line with the Disciplinary Policy and Procedure.

12.3 If a member of staff is subjected to, or knows about harassment, upskirting or bullying that has occurred via staff email or using School/Trust owned devices, they are encouraged to report this immediately to their line manager, the Headteacher, or the People Team.

13. Safety and Security

13.1 The School / Trust network will be secured using firewalls in line with the Data and E-Security Breach Prevention and Management Plan.

13.2 Filtering of websites, as detailed in the Data and E-Security Breach Prevention and Management Plan, will ensure that access to websites with known malware are blocked immediately and reported to the ICT department.

13.3 Approved anti-virus software and malware protection must be installed on all devices and will be updated automatically by the relevant servers.

13.4 The school will use mail security technology to detect and block any malware transmitted via email.

13.5 Members of staff must ensure that all School / Trust owned electronic devices are made available as and when required for anti-virus updates, malware protection updates and software installations, patches or upgrades.

13.6 Records will be kept detailing which devices have been issued to employees these will be stored in the ICT department.

13.7 Programmes and software must not be installed on School / Trust owned electronic devices without permission from the ICT department.

13.8 Staff are not permitted to remove any software from an electronic device without permission from the ICT department.

13.9 Members of staff who install or remove software from a School / Trust owned electronic device without seeking authorisation from the ICT department, may be subject to disciplinary measures.

13.10 All devices must be secured by a password or biometric access control.

13.11 System passwords must be kept confidential and must not be shared with pupils, unauthorised members of staff or third parties.

12.11 Personal passwords should not be shared with anyone, including the ICT department.

12.13 Devices must be configured so that they are automatically locked after being left idle for a set time of no more than five minutes for mobile and other portable devices and 10 minutes for desktop computers.

12.14 All devices must be encrypted.

12.15 Further security arrangements are outlined in the Data and E-Security Breach Prevention and Management Plan.

14. Loss, Theft and Damage

14.1 For the purpose of this policy, ‘damage’ is defined as any fault in a School or Trust owned electronic device caused by the following:

- Connections with other devices, e.g. connecting to printers which are not approved by the ICT department
- Unreasonable use of force
- Abuse
- Neglect

- Alterations
- Improper installation

14.2 The Trusts insurance cover provides protection from the standard risks whilst a School / Trust owned device is on the premises or in your home, but excludes theft from your car or other establishments. Should you leave a school device unattended and it is stolen, you will be responsible for its replacement and may need to claim this from your insurance company or pay yourself.

14.3 Any incident which leads to a School / Trust owned electronic device being lost is treated in the same way as damage.

14.4 The ICT department and headteacher will decide whether a device has been damaged due to the actions described above.

14.5 The ICT department will be contacted if a School / Trust owned electronic device has a technical fault and or damage: Repairs and replacements will be undertaken by the ICT department only.

14.6 If it is decided that a member of staff is liable for the damage, they are required to pay the total repair or replacement cost.

14.7 A written request for payment is submitted to the member of staff who is liable to pay for damages.

14.8 If the member of staff believes that the request is unfair, they can make an appeal to the headteacher, who makes a final decision within two weeks.

14.9 In cases where the headteacher decides that it is fair to seek payment for damages, the member of staff is required to make the payment within six weeks of receiving the request.

14.10 Payments are to be deducted from salary or other method as detailed below.

14.11 The Trust accepts payments made via credit and debit cards, cheques and cash.

14.12 The headteacher may choose to accept the payment in instalments.

14.13 The member of staff is not permitted to access school-owned electronic devices until the payment has been made.

14.14 In cases where a member of staff repeatedly damages school-owned electronic devices, the headteacher may decide to permanently exclude the member of staff from accessing devices.

14.15 If a School / Trust owned device is lost or stolen, or is suspected of having been lost or stolen, the DPO and ICT Technical Lead must be informed as soon as possible to ensure the appropriate steps are taken to delete data from the device that relates to the School, Trust, its staff and its pupils, and that the loss is reported to any relevant agencies.

14.16 The School / Trust is not responsible for the loss, damage or theft of any personal device, including phones, cameras, tablets, removable media, etc.

15. Remote Working

15.1 All of the points stated within this policy apply whilst working away from the office, or in a home environment

15.2 It is expected that staff working remotely will make all efforts to attend meetings as they would whilst attending the school or Trust offices.

15.3 Ensure you are available through remote communication methods during your working hours.
15.4 Dress appropriately and smartly as you would for working in the office.

15.5 Be aware of your surroundings – adjust your workspace so there is plenty of light and ensure the background of your room is appropriate.

15.6 Be mindful of any background noise from children, pets or any form of internal / external work in and around your house.

15.7 When not communicating for periods of time mute your microphone to help with background noise and feedback issues.

15.8 Stay seated and present in the meeting as you would in an office environment.

15.9 Try not to eat or drink during a virtual meeting or presentation.

16. Implementation

16.1 Staff are requested to report any breach of this policy to the headteacher or ICT Technical Lead.

16.2 Regular monitoring and recording of email messages will be carried out on a random basis. Hard copies of email messages can be used as evidence in disciplinary proceedings.

16.3 Use of the telephone system is logged and monitored.

16.4 Use of the school internet connection is recorded and monitored.

16.5 The ICT Department will conduct random checks of asset registered and security marked items.

16.6 The ICT department will if required check computer, server and network logs for misuse.

16.7 Unsuccessful and successful log-ons are logged on every computer connected to the School / Trust network.

16.8 Unsuccessful and successful software installations, security changes and items sent to the printer are also logged.

16.9 The ICT department can remotely view or interact with any of the computers on the network. This may be used randomly to implement this policy and to assist in any difficulties.

16.10 Anti-virus software is installed with a centralised administration package; any virus found is logged to this package and the ICT department alerted.

16.11 All users of school / Trust database systems will be issued with a unique individual password, which must be changed at regular intervals. Staff must not, under any circumstances, disclose this password to any other person, including other members of staff or ICT technicians.

16.12 Attempting to access the database using another employee's user account/password without prior authorisation is likely to result in disciplinary action, including summary dismissal.

16.13 User accounts are accessible to the ICT Department through the use of elevated rights, however no access will be made unless deemed necessary for support and approved by a member of SLT.

16.14 Users are required to be familiar with the requirements of the GDPR and Data Protection Act 2018, and to ensure that they operate in accordance with the requirements of the regulations and the Data Protection Policy.

16.15 Any breach of the rules in this policy may result in disciplinary action, which may lead to dismissal.

16.16 A misuse or breach of this policy could also result in criminal or civil actions being brought against the persons involved or the School / Trust.

17. Monitoring and Review

17.1 This policy will be reviewed annually by the ICT Technical Lead to determine if updates are required.

17.2 Any changes or amendments to this policy will be communicated to all staff members by the ICT Technical Lead.

17.3 This policy will be reviewed by Trustees on a three year cycle if not presented to them sooner.