EASTERN MULTI-ACADEMY TRUST

Group Policy Document

ICT Acceptable Use Policy

(including Internet, email and social media policy)

Summary

This policy outlines the use of academy ICT resources for staff, pupils, parents and governors to establish clear expectations for the way all members of the academy communities and Trust engage with each other online, in support of the Trust's policies on data protection, online safety and safeguarding.

This policy covers all users of our Trust's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

If you are unsure about the validity of the content of this policy please refer to the Policy Owner.

Please Note: This policy is applicable to All Employees / Teachers / Support Staff / Volunteers including Trustees and Governors within the Group.

Policy owner	**Audit Committee**
Policy holder	**Chief Executive Officer**
Author	David Cousins, Chief Finance Officer Rebecca Schrooder, Operations Manager
Policy Inventory ID Number	**DP17**
Group Policy Area	IT Security and GDPR Policies

Approved by

Consultation Group	**Audit**
Approval Committee	**Audit**
Implementation date	**July 2025**
Review Date	**July 2028**

Version Control

Control No	Change summary	Consultation Group	Effective date
01	Addition of section 11 on acceptable use of Artificial Intelligence and inclusion of AI to Appendix 2, 3, 4 & 5.	ELT Audit	July 2025

Contents

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our academies and Trust work, and is a critical resource for pupils, staff (including senior leadership teams), governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the academy and central Trust services.

However, the ICT resources and facilities our academies use also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of academy ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the academy community engage with each other online
- Support the Trust's policies on data protection, online safety and safeguarding
- Prevent disruption to the academy and Trust through the misuse, or attempted misuse, of ICT systems
- Support the academy in teaching pupils safe and effective internet and ICT use

This policy covers all users of our Trust's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

The Trust's ICT Facilities must only be used by those authorised to do so. Any user who requires access to Trust ICT Facilities must first:

- Be authorised to do so
- Read, understand and accept all relevant Trust policies, including this Acceptable Use Policy
- Sign and return the confirmation of Acceptable Use Policy – shown in Appendix 4

Breaches of this policy may be dealt with under our appropriate staff or pupil policies such as disciplinary policy/academy behaviour policy/staff discipline policy/staff code of conduct

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2024
- Searching, screening and confiscation: advice for academies
- National Cyber Security Centre (NCSC)

- Education and Training (Welfare of Children Act) 2021

  Information Commissioner's Office

- Guidance on the use of Cloud Computing
- Bring Your Own Device Guidance
- End User Device Guidance
- DfE Guidance on Generative AI in Education 2025
- JCQ Guidance on AI in Assessments 2024

3. Definitions

- **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service
- **"Users":** anyone authorised by the Trust to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **"Personal use":** any use or activity not directly related to the users' employment, study or purpose
- **"Authorised personnel":** employees authorised by the Trust to perform systems administration and/or monitoring of the ICT facilities
- **"Materials":** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 6 for a glossary of cyber security terminology.

4. Unacceptable use

The following is considered unacceptable use of the academy's ICT facilities by any member of the academy community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the academy's ICT facilities includes:

- Using the academy's ICT facilities to breach intellectual property rights or copyright
- Using the academy's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the academy's or Trust's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth-produced sexual imagery)
- Activity which defames or disparages the academy or Trust, or risks bringing the academy or Trust into disrepute

- Sharing confidential information about the Trust, the academy, its pupils, or other members of the academy or Trust community
- Connecting any device to the academy's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the academy's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the academy's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the academy
- Using websites or mechanisms to bypass the academy's filtering mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way

This is not an exhaustive list. The Trust reserves the right to amend this list at any time. The Principal or member of Trust Senior Leadership Team will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the academy's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of academy ICT facilities (on the academy/Trust premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Chief Executive Officer's discretion.

Please contact the CEO for permission.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the academy's policies on pupil behaviour, staff discipline/staff code of conduct.

5. Staff (including governors, volunteers, and contractors)

5.1 Access to Trust ICT facilities and materials

The Trust's IT provider manages access to the Trust and academy's ICT facilities and materials for staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the academy's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the IT services provider via their helpdesk: Raise a Support Ticket

Staff should:

- Make sure that at all times that this equipment is used appropriately, securely, for the purpose for which it was issued to you, without reconfiguration and in compliance with relevant legislation such as the Computer Misuse Act 1990 and Data Protection Act 2018
- On leaving the Trust, the user must ensure that all ICT equipment is returned
- Before the user stores any films, music or other media on ICT equipment, they must ensure that they are aware of their responsibilities under current Intellectual Property Legislation.
- Report the loss or theft of ICT Equipment to the Trust

5.1.1 Laptop, Tablet and Smartphone Users (for use on Trust premises and offsite remote working)

All Trust ICT equipment is subject to information security risks, but the portability of laptops, tablets and smartphones makes them particularly vulnerable to damage, loss or theft, either for their re-sale value or the information they contain. When outside of secured premises, there is an increased risk to any laptops or portable devices that a user may carry as part of their role.

- Users must keep ICT equipment in their possession within their sight whenever possible. ICT equipment should never be left visibly unattended unless it is suitably secured (for example in a secure office)
- Extra care should be taken in public places such as airports, railway stations or restaurants
- The user must ensure that the device is regularly connected and logged onto the network to receive its security updates at least monthly
- Any data saved to the device is not backed up centrally. The user should avoid saving data to the device wherever possible. However, where this is necessary for operational reasons the user must ensure that data on the device is backed up to the network storage areas for the Trust as soon as is practical.
- If a device is secured either with an encryption password or a 'lock screen' password, the user must not share your encryption or lock screen password with anyone nor write them down.

5.1.2 Use of phones and email

The academy provides each member of staff with an email address.

This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email accounts.

All work-related business should be conducted using the email address the academy has provided.

Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does

not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform their local data lead and report via GDPR Sentry immediately and follow our data breach procedure.

If a user receives an e-mail from an unknown source ('Spam' e-mail) they must not open any attachments or click on any links. They should neither forward the e-mail nor reply to the sender (as this may attract further e-mails).

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the academy to conduct all work-related business.

Academy phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

5.1.3 Secure Disposal of Trust ICT Equipment

Trust equipment which is broken, no longer fit for purpose or to be used/donated for other purposes should be returned to the IT department where it will be securely wiped (where applicable) and disposed in-line with regulations.

The user must not sell or donate Trust equipment to staff, charities or any third-parties without the explicit authorisation of the Trust's Chief Executive or Principal.

5.2 Personal use

The use of non-Trust and personal ICT equipment to undertake Trust business brings both opportunities and risks. The potential for an increase in flexibility and convenience must be balanced against the need to keep personal and sensitive information secure.

- The user must only use their personal handheld/external devices (mobile phones/USB devices etc.) to undertake Trust business in school if permission has been gained. Employees must understand that, if they do use their own devices in school, they will follow the rules set out in this agreement, in the same way as if they were using Trust equipment
- Users must keep personal phone numbers and email accounts private and not use their own mobile phones or email accounts to contact pupils
- Users must only use a Trust mobile phone to undertake Trust business when on a Trust trip other than in emergencies

Staff are permitted to occasionally use Trust ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The IT provider on instruction from Principals or Trust SLT may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time/teaching hours/non-break time
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the academy's ICT facilities to store personal non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the academy's ICT facilities for personal use may put personal communications within the scope of the academy's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff should be aware that personal use of ICT (even when not using academy ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents could see them.

Personal use of Trust ICT equipment does not extend to other family members, friends or any other person, unless formally authorised to do so by the Trust.

Staff should take care to follow the academy's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times.

The Trust has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

Although this Acceptable Use Policy applies to the use of Trust facilities, it is important to note that the use of Social Media outside of work can affect the workplace. For example, comments posted on Social Media may be seen by work colleagues, and a private disagreement may 'spill over' into the workplace;

- Users should follow the general principles of what is considered unacceptable use outlined in Section 4 of this document
- A user must not use social networking sites to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages
- A user must not befriend pupils on social networking sites. (Staff should consider carefully the implications of befriending parents or ex-pupils)
- A user should not post information and photos about themselves, or Trust-related matters, publicly that they wouldn't want employers, colleagues, pupils, parents and other Trust stakeholders to see

Academies have official Facebook/Twitter pages, managed by the Principal or their delegate. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The academies have guidelines for what can and cannot be posted on their social media accounts. Those who are authorised to manage those account must ensure they abide by these guidelines at all times.

5.3 Remote access

We allow staff to access the academy's ICT facilities and materials remotely.

Staff accessing the academy's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the academy's ICT facilities outside the academy and take such precautions as the Trust or IT Service provider may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

5.5 Monitoring of academy network and use of ICT facilities

The academy reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The academy monitors ICT use in order to:

- Obtain information related to academy business
- Investigate compliance with academy policies, procedures and standards
- Ensure effective academy and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

6. Pupils

6.1 Access to ICT facilities

- Computers and equipment in the academy's ICT suite are available to pupils only under the supervision of staff
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the academy has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under academy rules or legislation.

The academy can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the academy's rules.

Staff members may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse contains an online element.

6.3 Unacceptable use of ICT and the internet outside of academy

The academy will sanction pupils, in line with the academy behaviour policy, if a pupil engages in any of the following **at any time** (even if they are not on academy premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the academy's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the academy, or risks bringing the academy into disrepute
- Sharing confidential information about the academy, other pupils, or other members of the academy community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the academy's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

7. Parents

Access to ICT facilities and materials

Parents do not have access to the academy's ICT facilities as a matter of course.

However, parents working for, or with an academy in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the academy's facilities at the Principal's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

8. Data security

The Trust is responsible for making sure they have the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, the Trust cannot guarantee security. Staff, pupils, parents and others who use the Trust's ICT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the academy's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

All staff will store their passwords securely, if required. Our systems will require regular password updates, users will receive notifications at log in when they need to reset their password.

8.2 Software updates, firewalls and anti-virus software

All of the Trust's ICT devices that support software updates, security updates and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the Trust's ICT facilities.

Any personal devices using the academy's network must all be configured in this way.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the Trust's data protection policy.

8.4 Access to facilities and materials

All users of the academy's ICT facilities will have clearly defined access rights to academy systems, files and devices.

These access rights are managed by our IT service provider.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert their line manager immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

8.5 Encryption

The Trust ensures that its devices and systems have an appropriate level of encryption.

Staff may only use personal devices (including computers and USB drives) to access academy data, work remotely, or take personal data (such as pupil information) out of academy if they have been specifically authorised to do so by the Principal.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by our IT service provider.

8.6 Cloud Services

The terms 'Cloud Services' or 'The Cloud' cover a number of technologies which provide access to software, applications, data and ICT infrastructure (typically) over the Internet. For example, services such as Dropbox offer file storage; Office 365 allows access to e-mail and Microsoft Office applications.

The UK Government and the Information Commissioner's Office have issued guidance about the use of 'Cloud'. Links to this guidance can be found in Section 2.

We encourage staff to make use of Cloud-based technologies approved by the Trust for sharing information and collaborating; however, a user must not store any sensitive Trust information in a Cloud Service which has not been formally assessed and approved by the Trust for that purpose.

8.7 Data Security Incidents

A successful compromise may:

- affect business operations and lead to financial loss or reputational damage
- be a threat to the personal safety or privacy of an individual
- need to be reported to the UK Government, the Information Commissioner's Office, the Police or a number of other organisations

Therefore, don't ignore a data security incident assuming that someone else will report it, ensure all data security incidents are reported via GDPR Sentry without delay.

Examples of security incidents:

- Damage to or theft/loss of information (either manual or electronic)
- The finding of confidential information/records in a public area
- Poor disposal of confidential waste
- Unauthorised access to information
- Unauthorised disclosure of confidential information to a third party (in any format including verbally)
- Transfer of information to the wrong person (by email, fax, post, or phone)
- Receiving of information (such as by email or fax) meant for someone else
- Sharing of computer IDs and passwords
- Loss or damage to paper-based files containing sensitive or personal identifiable information
- Loss of computer equipment due to crime or an individual's carelessness
- Loss of computer media e.g. CD, USB stick
- Corrupted data
- Access to inappropriate websites in breach of policy
- Theft

- Fraud
- A computer virus
- Successful hacking attack

9. Protection from cyber attacks

Please see the glossary (appendix 5) to help you understand cyber security terminology.

The Trust will:

- Work with governors and the IT provider to make sure cyber security is given the time and resources it needs to make the academy secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the academy's annual training window) on the basics of cyber security.
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Back up critical data daily and store these backups on systems/external hard drives that aren't connected to the academy network and which can be stored off the academy premises
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our IT Service provider.
- Make sure staff:
    - Enable multi-factor authentication where they can, on things like academy email accounts
    - Store passwords securely using a password manager
- Make sure our IT provider conducts regular access reviews to make sure each user in the academy has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and seeing if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT provider, for example, including how the academy will communicate with everyone if communications go down, who will be contacted when, and who will notify Action Fraud of the incident. This will be reviewed and tested regularly and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

10. Internet access

The academies wireless internet connection is secured.

- We use filtering
- Sometimes we have separate connections for staff/pupils/visitors

If you need to report inappropriate sites that the filter hasn't identified (or appropriate sites that have been filtered in error) please contact our IT service provider via the helpdesk.

Staff must not give the wifi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. Artificial Intelligence

Artificial Intelligence (AI) is increasingly being used across education to support teaching, learning, and administration. EMAT recognises the opportunities AI presents for enhancing efficiency and innovation. However, AI must be used in a safe, ethical, and responsible manner, ensuring compliance with safeguarding, data protection, and academic integrity principles.

11.1 Leadership and Governance

- Trust leaders play a vital role in overseeing AI governance, ensuring policies align with national regulations, and implementing best practices for safe and ethical AI use.
- Ensure AI governance aligns with DfE, KCSIE, and GDPR regulations (this policy does).
- Approve AI tools before they are used in teaching, learning, or administration.
- Ensure AI use is transparent, fair, and free from bias.
- Engage in update training to ensure compliance and risk mitigation for the latest risks from AI

11.2 Teaching and Support Staff

- Teachers and support staff are responsible for ensuring AI is used as an educational aid while maintaining academic integrity, supporting student learning, and preventing misuse.
- Use AI as a teaching aid, not as a replacement for pedagogy.
- Verify AI-generated content for accuracy, appropriateness, and bias.
- Educate students on AI literacy, misinformation, and deepfakes.
- Ensure AI use does not compromise academic integrity or safeguarding.

11.3 Students

- Students must develop an understanding of AI's capabilities and limitations while using AI tools ethically and responsibly within the guidelines set by the academy.
- Use AI tools responsibly and in line with Academy or Trust policies.
- Declare AI use in coursework, assignments, and assessments where required.
- Understand ethical considerations and avoid over-reliance on AI.

11.4 IT and Data Protection Teams

- The IT and Data Protection teams are responsible for ensuring AI systems comply with data protection laws, cybersecurity standards, and safeguarding requirements.
- Implement security measures to ensure AI tools comply with data protection laws.

- Ensure that AI tools used in academy settings do not process or store personal data without anonymisation.
- Conduct regular cybersecurity audits to monitor AI-related risks.
- Engage in update training to ensure compliance and risk mitigation for the latest risks.

11.5 Ethical AI Use

AI should be implemented in ways that are fair, transparent, and aligned with ethical considerations. This section outlines the key principles for ensuring AI use remains accountable, unbiased, and secure.

11.5.1 Transparency and Accountability

- It is essential that AI use within the school remains transparent, and that decisions made using AI are documented and subject to human oversight.
- AI must not be used to make independent decisions affecting students or staff.
- The use of AI in assessment, recruitment, or administrative decision-making must be documented.
- AI-generated content must be identified where used.

11.5.2 Bias and Fairness

- AI systems must be reviewed and monitored to minimise bias, ensuring fairness in learning, assessment, and administrative decision-making.
- AI tools must be vetted to ensure fairness and prevent bias.
- Training must be provided to recognise AI bias and hallucinations and mitigate its impact.
- Human checking is required for all AI output.
- All stakeholders are responsible for any output shared that has been generated by AI.

11.5.3 Data Protection and Anonymisation

- To comply with data protection regulations, AI tools must not process personal data unless approved. Where possible, anonymisation techniques should be used to protect individual privacy.
- AI tools must not process or store personally identifiable student or staff data unless explicitly approved by the IT and Data Protection teams.
- AI inputs should be anonymised where possible.
- A Data Protection Impact Assessment (DPIA) must be conducted before new AI tools are introduced. Colleagues are NOT allowed to use any new software without prior permission from the IT and Data Protection team.

11.6 AI in Assessments and Academic Integrity

AI must not compromise academic integrity and EMAT will ensure that students and staff adhere to fair assessment practices while using AI tools appropriately.

11.6.1 Preventing AI Misuse in Assessments

- To maintain assessment integrity, students must declare AI-assisted work, and staff must monitor submissions for signs of unauthorised AI use.

- AI must not be used to generate coursework, essays, or exam content.
- Students must declare any AI-assisted work in line with JCQ and school regulations.
- Staff must monitor for sudden changes in student work that suggest AI misuse e.g. work that is suddenly better than previously seen, Americanisation of language, other hallmarks of AI-generated content.

11.7. Safeguarding and Online Safety

AI must be used safely within the school environment, preventing harm and ensuring students and staff understand the potential risks associated with AI-generated content.

11.7.1 Preventing AI-Generated Harm

AI-generated content, including deepfakes and misinformation, presents new safeguarding challenges.

- Staff and students must be aware of these risks and trained to respond appropriately.
- AI tools must not be used to create harmful, misleading, or inappropriate content.
- Students and staff must be trained to recognise AI-generated deepfakes, misinformation, and impersonation risks.
- The Trust's filtering and monitoring systems must detect and prevent AI-generated threats (as per the Government's Filtering and Monitoring standards).

11.7.2 AI and Cybersecurity

- As AI systems become more integrated into school operations, cybersecurity risks must be managed to prevent unauthorised access, phishing attempts, and data breaches.
- AI-related phishing scams, fraud, and cybersecurity risks must be monitored.
- IT teams must ensure AI tools do not introduce security vulnerabilities.

12. Monitoring and review

The Principal, Trust leadership and IT service provider monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the academy.

This policy will be reviewed every 3 years.

13. Related policies

This policy should be read alongside the academy or Trust's policies on:

E-safety

IT Security

Safeguarding and child protection

Behaviour

Staff Code of Conduct

Disciplinary Policy

Data Protection

Appendix 1: Facebook cheat sheet for staff

Don't accept friend requests from pupils on social media

10 rules for academy staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during academy hours
7. Don't make comments about your job, your colleagues, our academy or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the academy on your profile (e.g. by setting it as your workplace, or by 'checking in' at an academy event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if…

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the academy
    - Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: Acceptable use agreement for older pupils

Acceptable use of the academy's ICT facilities and internet: agreement for pupils and parents/carers	
Name of pupil:	
When using the academy's ICT facilities and accessing the internet in academy, I will not: • Use them for a non-educational purpose • Use them without a teacher being present, or without a teacher's permission • Use them to break academy rules • Access any inappropriate websites • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) • Use chat rooms • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo • Share my password with others or log in to the academy's network using someone else's details • Bully other people • Use AI tools responsibly and in line with Academy or Trust policies. • Not use AI to generate coursework, essays, or exam content and declare AI use in coursework, assignments, and assessments, where allowed. I understand that the academy will monitor the websites I visit and my use of the academy's ICT facilities and systems. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the academy's ICT systems and internet responsibly. I understand that the academy can discipline me if I do certain unacceptable things online, even if I'm not in academy when I do them.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the academy's ICT systems and internet when appropriately supervised by a member of academy staff. I agree to the conditions set out above for pupils using the academy's ICT systems and internet, and for using personal electronic devices in academy, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: Acceptable use agreement for younger pupils

Acceptable use of the academy's ICT facilities and internet: agreement for pupils and parents/carers	
Name of pupil:	
When I use the academy's ICT facilities (like computers and equipment) and get on the internet in academy, I will not: • Use them without asking a teacher first, or without a teacher in the room with me • Use them to break academy rules • Go on any inappropriate websites • Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson) • Use chat rooms • Open any attachments in emails, or click any links in emails, without checking with a teacher first • Use mean or rude language when talking to other people online or in emails • Send any photos, videos or livestreams of people (including me) who aren't wearing all of their clothes • Share my password with others or log in using someone else's name or password • Bully other people • Use AI tools without permission of my teacher I understand that the academy will check the websites I visit and how I use the academy's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules. I will tell a teacher or a member of staff I know immediately if I find anything on a academy computer or online that upsets me, or that I know is mean or wrong. I will always be responsible when I use the academy's ICT systems and internet. I understand that the academy can discipline me if I do certain unacceptable things online, even if I'm not in academy when I do them.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the academy's ICT systems and internet when appropriately supervised by a member of academy staff. I agree to the conditions set out above for pupils using the academy's ICT systems and internet, and for using personal electronic devices in academy, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 4: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of Trust ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

To ensure that members of staff are fully aware of their professional responsibilities when using ICT systems and equipment, staff are required to sign this document.

Members of staff must read and understand the Trust's IT Security Policy, E-Safety Policy and the Acceptable use of ICT Policy prior to signing.

Name of staff member/governor/volunteer/visitor:

I understand that the Trust's ICT equipment is the property of the Trust whether used on or off the premises.

I understand that the Trust's ICT systems and services must be used in accordance with Trust policies whether used on or off the premises.

I understand that it is a disciplinary offence to use any Trust ICT system, services or equipment for a purpose not permitted by the Trust. This includes (but is not limited to):

- conducting illegal activities
- accessing or downloading pornographic material
- political purposes
- gambling
- soliciting for personal gain or profit
- managing or providing a business service using the Internet
- advertising
- revealing or publicising proprietary or confidential information
- representing personal opinions as those of the Trust, or saying to speak on behalf of the Trust
- making or posting indecent remarks or proposals
- sending chain letters
- using software in violation of its copyright
- Illegal downloading from torrent sites (copyright music and films etc.)
- intentionally interfering with the normal operation of Trust Internet services, Learning Platform services, Management Information System, hardware or software

(Staff are permitted to browse the internet and undertake activities such as online shopping during non-contact time (teachers) or designated breaks (support staff)).

I understand that my use of Trust systems, software, Internet and email is monitored and recorded to ensure policy compliance. Where the Trust believes that unauthorised use of equipment, systems or services may be taking place, it may delete inappropriate materials and may take disciplinary action. Where the Trust believes that equipment, systems or services may be being used for unlawful or criminal purposes this may be referred to the appropriate agency.

I accept that I am responsible for the use and protection of the user credentials with which I am provided (user account and password, access token or other items I may be provided with)

I will not attempt to access any computer system to which I not been given access. I will respect system security and I will not disclose or share any login, password or security information to anyone other than an authorised system manager. I will not use anyone else's user account and password to access company systems

I will protect any sensitive material sent, received, stored or processed by me according to the level of classification assigned to it, including both electronic and paper copies

I will not send classified or sensitive information over the Internet via email or other methods unless appropriate methods (e.g. encryption) have been used to protect it from unauthorised access

I will always ensure that I enter the correct recipient email address(es) so that sensitive information is not compromised

I will ensure I am not overlooked by unauthorised people when working and will take appropriate care when printing sensitive information

I will securely store sensitive printed material and ensure it is correctly destroyed when no longer needed

I will not leave my computer unattended such that unauthorised access can be gained to information via my account while I am away

I will make myself familiar with the organisation's security policies and procedures and any special instructions relating to my work

I will inform my manager immediately if I detect, suspect or witness an incident that may be a breach of security

I will not attempt to bypass or subvert system security controls or to use them for any purpose other than that intended

I will not remove equipment or information from the organisation's premises without appropriate approval

I will not introduce viruses or other malware into the system or network

I will not attempt to disable anti-virus protection provided at my computer

I will comply with the legal, statutory or contractual obligations that the organisation informs me are relevant to my role

On leaving the organisation, I will inform my manager prior to departure of any important information held in my account

I understand that ICT includes a wide range of systems, includes but it not limited to: mobile phones, digital cameras, email and social networking. ICT use may also include personal ICT devices with the permission of the Principal if used for Trust business.

I understand that I must not communicate with current students of the Trust via public social networking sites (e.g. Facebook, Twitter, Instagram) and that if contact is required, I must use Trust-owned equipment or facilities (e.g. the email facility on the Learning Platform or MIS or a phone provided by the Trust).
I understand that my use of social networking sites (e.g. Facebook, Twitter, Instagram) should be for personal use only; however, should there be a requirement to use Social Media for Trust purposes then my usage will be consistent with my professional role. All communication with parents of students at the Trust should be conducted using Trust-owned equipment or facilities (e.g. the email facility on the Learning Platform, MIS or a phone provided by the Trust).

I understand that my use and storage of photographic images or video recordings of pupils taken in Trust or on Trust activities should be with parental/student consent.

I understand that any official Trust blogs, wikis, discussion boards etc. should be hosted on the Trust's website or Learning Platform, sharepoint/intranet.

I will respect and abide by all copyright and intellectual property rights.

I will ensure that all Trust electronic communications that I make are compatible with my professional role and Trust policies and will not use inappropriate humour, graphics or images.

I will seek to ensure that I check my email inbox each working day and deal with emails promptly and I will maintain my user area(s) in good order whether on a laptop or on networked computers or other devices.

I will ensure that students are appropriately supervised when using ICT equipment and remind them that their ICT activity is routinely monitored.

I will ensure that I will use AI tools ethically and in line with Academy or Trust policies, ensuring that AI use does not compromise academic integrity or safeguarding.

I will take all steps necessary for the protection of both IT and information whilst it is in my possession and I will also ensure that I either log off my computer or apply the screen lock should I need to leave the computer for any reason.

I will ensure that personal data is stored securely and is used appropriately, whether in Trust, taken off the Trust premises or accessed remotely. I will ensure that personal or confidential information is not stored on any computers not belonging to the Trust or on removable media, such as memory sticks, CDs etc except for the purpose of transfer of data from one Trust's computer to another Trust's computer, using encryption. I will ensure that no personal data is copied unless there is a specific legitimate requirement to do so.

I understand that computers provided by the Trust for use away from the Trust premises may be used for personal purposes provided that any usage does not constitute a breach of this or any other Trust policy or Code of Conduct.

I will not install any software or hardware without authorisation by the Principal or Trust's Chief Finance Officer

.

If using a computer provided by the Trust away from Trust premises, I will ensure that appropriate physical security measures are in place to safeguard the equipment. I will also ensure that any anti-virus protection software is updated prior to leaving the Trust.

I will report any information breach and/or security incidents of concern relating to the inappropriate use of ICT systems or equipment to the Academy or Trust Data Lead, the Designated Child Protection coordinator or Principal.

I have read, understood and accept the obligations outlined above for Acceptable Use of ICT.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Please sign and return to your Academy Principal or HR within one week of receipt

Appendix 5: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the academy will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Artificial Intelligence (AI)	Artificial intelligence (AI) describes computer systems which can perform tasks usually requiring human intelligence. This could include visual perception, speech recognition or translation between languages.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.

TERM	DEFINITION
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programs designed to self-replicate and infect legitimate software programs or systems.
Virtual Private Network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly targeted phishing attacks (where emails are made to look legitimate) aimed at senior executives.