ICT Policy

Academy Transformation Trust

Review Date

August 2025

Ratified

August 2025

Next Review Date

August 2028

Responsible Directorate

Operations (ICT)

Our Trust

These four critical questions make it clear who we are and what we do.
We ask ourselves these questions to guide our work and our improvement.

Why do we exist?

To **transform life chances** by achieving the highest possible standards and preparing all our students to lead successful lives.

How do we behave?

- **Hard work**
  We are determined to see things through to the end and are resilient when faced with challenges.
- **Integrity**
  We do the right thing because it is the right thing to do.
- **Teamwork**
  We work together to help everyone succeed.

What do we do?

- We educate, safeguard and champion all our learners.
- We set high standards for ourselves and our learners.
- We build the powerful knowledge and cultural capital which stimulates social mobility and lifelong learning.

How will we succeed?

1. Aligned autonomy
2. Keeping it simple
3. Talent development

Contents

Statement of Intent

As the world becomes more digitally connected, the use of ICT is an ever-increasing part of daily life in our trust, and its power is immense. If used incorrectly, it has unintended consequences. This policy seeks to ensure all stakeholders trust-wide use ICT responsibly, safely and with due care and attention.

We have a duty of care to ensure that all our pupils are competent, informed, safe users of ICT and web-based resources. Understanding online safety is a life skill and empowering children from an early age to safeguard themselves and their personal information must be nurtured throughout their education to see them into adult life.

We are committed to supporting teachers and parents to understand what safe internet use means, to identify and prevent potential risks and identify indicators of abuse and therefore ensure that all colleagues receive online safety training annually.

1 Introduction and Intent

1.1 ICT is an integral part of the way our academies work, and is a critical resource for pupils, colleagues, non-executives, volunteers, and visitors. It supports teaching and learning, operations, pastoral, and administrative functions across our Trust.

1.2 ICT resources and facilities our Trust use also pose risks to data protection, online safety and safeguarding.

1.3 This policy aims to:

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

This policy covers all users to our ICT facilities, including non-executives, colleagues, pupils, volunteers, contracts and visitors.

Breaches of this policy may be dealt with under our *Disciplinary Policy, Behaviour Policy, Code of Conduct,* or other policies and procedures.

2 Definitions

2.1 ***ICT Facilities –*** includes all facilities systems and services including but not limited to network infrastructure, user accounts, 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.

2.2 ***ICT Monitoring –*** is used for safety and security and all ICT monitoring is covered by Data Protection Impact Assessment (DPIA).

2.3 ***Users –*** anyone authorised by the Trust to use the ICT facilities, including governors, staff, pupils, volunteers, contractors, and visitors.

2.4 ***Social Media –*** may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.

2.5 ***Personal Use*** – any use or activity not directly related to the users' employment, study, or purpose.

2.6 ***Authorised Personnel*** – employees authorised by the academy/our Trust to perform systems administration and /or monitoring of the ICT facilities.

2.7 ***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.

2.8 ***Online Safety*** – Using ICT facilities and web-based resources to communicate or access information

3 Safeguarding Roles and Responsibilities

3.1 The Designated Safeguarding Lead (DSL) is a member of the academy senior leadership team and holds the strategic oversight to ensure that safeguarding, including online safety is effective. Please contact this person first or their Deputy via the academy if you have any concerns about a child or the online safety provision within the academy.

3.2 The **Local Governing Board** will:

- Maintain their statutory responsibility for monitoring the academy's approach to online safety as part of their overall safeguarding duties.
- The Governor with responsibility for safeguarding should include the governance of online safety within their role and they will:
- Keep up to date with emerging risks, online harms and threats including exploitation, online sexual harassment, radicalisation, and extremism through technology use
- Receive regular updates from the Principal/DSL regarding training, identified risks and incidents
- Monitor and ensure the effectiveness of online safety training within the academy
- Recommend further initiatives for online safety training and awareness within the academy.

- The nominated Safeguarding governor can also be contacted via the academy.

3.3 The **Principal** will:

- Have overall responsibility for online safety within their academy (the DSL will retain strategic oversight of online safety as part of their wider strategic leadership of safeguarding).
- Ensure all aspects of technology within the academy meet the online safety requirements within this policy.
- Delegate the responsibility for the technical elements of online safety to a member of ICT Support staff. The member of staff with responsibility for the technical elements of online safety will be known as ICT Support for the purposes of this policy.
- Ensure online safety training throughout the academy is planned and up to date and appropriate to the recipient (e.g., all staff, pupils, Senior Leadership Team (SLT), LGB and parents).
- Ensure that the DSL has received appropriate CPD to undertake their duties and that annual and ongoing online safety training is arranged for all staff, in line with core safeguarding training, and that new guidance is shared.
- Ensure that all online safety incidents are dealt with appropriately and promptly in accordance with academy safeguarding procedures and that records are kept including details of the incident and action taken.
- Ensure that online safety is appropriately addressed for all pupils through the curriculum.
- Ensure parents and carers are informed of what the academy staff are asking pupils to do online, including the sites they need to access and with whom they will be interacting online.

3.4 The **DSL** will:

- Keep up to date with the latest risks to children whilst using technology.
- Review the policy regularly and bring any matters to the attention of the Principal.
- Advise the Principal on online safety matters.
- Engage with parents and the academy community on online safety matters within the academy and/or at home.
- Liaise with ICT Support, central safeguarding team and other agencies as required.
- Keep a log of all online safety incidents; ensure staff know what to do if an incident is reported by our safeguarding software and ensure an effective response and appropriate audit trail.
- Ensure technical online safety measures within the academy are fit for purpose (e.g., internet filtering software; CPOMS, behaviour management software).
- Ensure appropriate reporting procedures are in place (e.g., reporting function of internet filtering/monitoring software).
- Ensure that all colleagues and volunteers will participate in online safety training as part of their annual core safeguarding training. Colleagues will also receive updates throughout the year from the DSL.

3.5 **ICT Support** will:

- Be responsible for ensuring that the ICT technical infrastructure is secure and monitored; this will include ensuring the following:
- Ensure the anti-virus is fit-for-purpose, up to date and applied to all capable devices

- Ensure the operating system updates are regularly monitored, and devices updated as appropriate
- Have access to Microsoft 365 audit records for a 12-month period. Other data will be held in line with our Data Retention and Disposal Schedule which is available in the Records Management Policy.
- Ensure any online safety technical solution such as internet filtering or monitoring are operating correctly
- Ensure the filtering levels are applied appropriately and accordingly to the age of the user and that categories of use are discussed and agreed with the DSL and Principal
- Ensure passwords are applied to **all** users regardless of age and are changed regularly. Passwords should be a minimum of eight characters for staff and secondary aged pupils.
- Ensure the Administrator account sets a strong password which is changed regularly and not reused within 12 months. The password must have at least eight characters, upper- and lower-case letters, numbers, and symbols.
- Use a standard user account that does not have administration privileges for day-to-day activities. They will also have access to an account with administrative privileges, and this will only be used to install software/performing network administration tasks.
- To always operate with integrity and never abuse the position of trust that administrators are placed in.

3.6 **All Colleagues** will ensure that:

- **They read and sign the Acceptable Use Agreement (Appendix 1)**
- They are aware that the use of equipment and software connected to the network is monitored and that concerns are reported to the principal.
- They have completed online safety training and receive updates.
- All details within the policy are understood and any uncertainty should be discussed with the DSL and/or Principal.
- Any pupil related online safety incident is reported to the DSL via CPOMS or the Principal if the matter is adult related.
- Promoting and sharing online safety practices are planned for and embedded into the curriculum.

3.7 **Pupils** will:

- Understand the boundaries for the use of Academy Transformation Trust ICT equipment and services. **These are given in the Acceptable Use Agreement for Pupils which all pupils must sign (Appendix 2 or 3);** failure to sign this agreement or breaking the agreement will likely result in access being denied to academy ICT facilities.
- Understand that any deviation or misuse of ICT equipment and/or services will be dealt with in accordance with the Behaviour Policy.
- Be aware that all devices are monitored through our safeguarding software and concerns shared with the safeguarding team or Principal.
- Understand that online safety is embedded into the curriculum. Pupils will be given appropriate advice and guidance by staff and should ask questions or ask for support as needed.
- Be fully aware how they can report areas of concern or safety concerns including sexual exploitation or harassment and extremism within or outside the academy.

3.8 **Parents and carers** will:

- Play the most important role in the development of their children, and as such we will actively support parents and carers in obtaining the skills and knowledge that they need to ensure the safety of pupils outside the academy environment.
- Be aware that all academy devices (inside the academy or lent to pupils to use at home) are monitored using software and by an external company and any concerns are reported to the DSL or Principal.
- Understand the academy needs to have procedures in place to ensure that their children can be properly safeguarded. As such, parents and carers will receive a copy of the *Acceptable Use Agreement for Pupils*.
- Support the academy when sanctioning pupils for compromising the online safety of themselves or others.

4 Unacceptable Use

4.1. The following is considered unacceptable use of our ICT facilities by any member of the Trust. Any breach of this policy may result in disciplinary or behaviour proceedings.

4.2. Unacceptable use of our ICT facilities includes:

- Using the ICT facilities to breach intellectual property rights or copyright
- Using the ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the 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
- Activity which defames or disparages our Trust, or risks bringing us into disrepute
- Sharing confidential information about the academy, its pupils, or other members of the academy community or the Trust
- Connecting any device to the ICT network without approval from authorised personnel
- Setting up any software, applications, or web services on the 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 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
- Using websites or mechanisms to bypass the Trust's filtering mechanisms

4.3. This is not an exhaustive list. We reserve the right to amend this list at any time. The Principal or any other relevant member of staff will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the ICT facilities.

4.4. Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with our policies on behaviour/disciplinary/code of conduct.

5 Staff

5.1. Where this policy refers to staff, this refers to governors, volunteers, and contractors in addition to employees of our Trust

5.2. The academy ICT Support team manages access to the ICT facilities and materials for staff. That includes, but is not limited to:

- Computers, tablets and other devices
- Access permissions for certain programs or files

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

5.4. 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 ICT Support team by creating a support ticket via the ICT helpdesk system.

5.5. The Trust provides each member of staff with an email address using Microsoft 365. This email account should be used for work purposes only. Using a personal device to access work email or other data is allowed, providing security mechanism is in place on the device such as PIN number, passwords, facial recognition, fingerprint etc.

5.6. Staff should be extra vigilant when opening emails/clicking on links as they could be phishing emails or contain viruses.

5.7. Staff will receive annual Cyber Security Training which will cover phishing awareness and AI misuse.

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

5.9. 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.

5.10. 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.

5.11. Email and other digital communication messages are required to be disclosed in legal proceedings or in response to requests from individuals under the *Data Protection Act* (2018) (GDPR) in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purpose of disclosure. All email messages should be treated as potentially retrievable.

5.12. Staff must take extra care when sending sensitive or confidential information by email. Rather than sending attachments it is safer to store the file in a central location such as SharePoint or OneDrive and then securely share the file with the intended recipients.

If this is not possible, you should consider encrypting the email and its attachments if this contains sensitive or confidential information to ensure this is only accessible by the intended recipients. Staff can contact the ICT Support Team if they are unsure how to do this.

5.13. 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.

5.14. If academy staff send an email in error which contains the personal information of another person, they must inform the ICT Support Team and the Data Protection Lead immediately (who will inform the Data Protection Officer) and follow our *Data Breach Procedure*. Other staff should inform the Central ICT Team and the Data Protection Officer immediately.

5.15. Phones must not be used for anything that contravenes this policy

5.16. Academies may have the ability to record in-coming and out-going phone conversations. If calls are recorded, the caller must be made aware of this and the reasons why they are being recorded.

5.17. 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 ICT Support team or Principal may withdraw permission for it any time or restrict access at their discretion. Personal use is permitted if it:

- 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

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

5.19. Staff should be aware that use of the ICT facilities for personal use may put personal communications within the scope of the ICT monitoring activities (See Section 8.7). Where breaches of this policy are found, disciplinary action may be taken.

5.20. Staff are also permitted to use their personal devices (such as desktop computer, laptop, mobile phone or tablet) if security mechanisms are in place – see Section 5.5 and in line

with our Staff Code of Conduct. If you choose to do this, and you share your device and/or password with another person, you must logout of your Trust account first.

5.21. Staff should take care to follow the Trust guidelines on social media and use of email/digital communication to protect themselves online and avoid comprising their professional integrity.

5.22. We may provide remote access that allows staff to access Trust ICT facilities and materials remotely. This allows staff to login from home and access the ICT facilities such as, user area and shared areas. Remote access is managed by the ICT Support team.

5.23. If staff are using personal devices to work from home, they must be particularly vigilant and ensure they have up to date anti-virus software installed on their computer and take such precautions to protect the ICT facilities from importing viruses or compromising system security.

5.24. 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.

5.25. The Trust 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

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

5.27. The Trust monitors ICT use to:

- Obtain information related to academy business
- Investigate compliance with policies, procedures, and standards
- Ensure the ICT facilities are operating correctly
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a Subject Access Requests, Freedom of Information Act requests, or any other legal obligation.

6 Pupils

6.1 Pupils will have access to a range of ICT facilities within the academy. ICT facilities in the academy are only available to pupils under the supervision of staff. Post-16 pupils may use computers independently for educational purposes only.

6.2 Under the *Education Act (2011)*, and in line with the Department of 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.

6.3 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 rules.

6.4 The academy will sanction pupils, in line with the 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/Trust policies and 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
- Activity which defames or disparages our Trust, 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 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
- Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the academy policies on behaviour/staff discipline/staff code of conduct

7 Parents

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

7.2 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 ICT 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.

7.3 We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online. Parents play a vital role in helping model this behaviour for their children, especially when communicating with an academy through our website and social media channels.

8 Online Safety Technology

8.1 We use a range of ICT software and systems to safeguard pupils/staff and prevent loss of personal data. The following assistive technology is employed:

8.2 **Internet Filtering:** software is used to prevent access to illegal or inappropriate websites. What is appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. Filtering providers are members of the Internet Watch Foundation and systems block access to illegal Child Abuse Images and Content (CAIC). Filtering systems include the police assessed list of
unlawful terrorist content, produced on behalf of the Home Office Systems. They are used to monitor and report online activity including email and website access in multiple languages.
The DSL and ICT Support are responsible for ensuring that filtering is appropriate and that any issues are brought to the attention of the Principal. The academy can determine the level of
filtering at network level, to be age and group appropriate and to permit and deny content as require (this may be through third party support).

8.3 **Network Monitoring:** monitoring software allows the tracking and reporting of incidents to safeguard users. If an academy/Trust device is used through the academy network and off site, it will be monitored. Monitoring occurs whilst using any aspect of the network and is not restricted to online use.

8.4 **Reporting:** the academy provides the ability to report inappropriate content. Incidents are logged and shared with the DSL and/or SLT as appropriate. A log of website activity is kept.

8.5 **Email Filtering:** every effort will be made to ensure emails are not infected including the use of software that prevents infected emails being sent from or received by the academy. Emails are monitored for inappropriate content.

8.6 **Encryption:** all academy devices that hold personal data (as defined by the *Data Protection Act (2018)* are encrypted. No data is to leave the academy on an un-encrypted device. All devices that are kept on academy property and which may contain personal data are

encrypted. Any breach (e.g., loss/theft of a device such as a laptop or USB key drives) is to be brought to the attention of the Principal and ICT Support who will act accordingly.

8.7 **Passwords:** staff and pupils will be unable to access any device without a unique username and password. Staff and pupil passwords will change on a regular basis. ICT Support will be responsible for ensuring that passwords are changed.

8.8 **Anti-Virus:** all capable devices will have anti-virus software. This software will be regularly updated for new virus definitions. ICT Support will be responsible for ensuring this task is carried out and will report to the Principal if there are any causes for concern. All USB peripherals such as key drives (if allowed) are to be scanned for viruses before use.

8.9 **Internet:** use of the internet in the academy is a privilege, not a right. Internet use will be granted to staff, volunteers, and pupils upon completion of training and on signing the appropriate *Acceptable Use Agreement.*

8.10 **Cyber Security:** all users will be extra vigilant when clicking on website/email (phishing) links of unknown or suspicious sources as this could cause a cyber security breach. Discuss with the ICT Support team if unsure.

8.11 **Email:** all staff are reminded that emails are subject to Freedom of Information requests, this means emails should be of a professional, work-based nature and as such, written appropriately. Emails of a personal nature are not permitted. Pupils are permitted to use the email system and as such will be given their own email address.

8.12 **Photos and Videos:** parents should sign a digital media (such as photos and videos) consent form on the pupil's entry to the academy, including Early Years. Non-return of the consent form will not be presumed as consent.

8.13 **Mobile Phones and Hand-Held Electronic Devices:** Pupils will only use their mobile phones in line with the acceptable use agreement and academy rules specifically on the use of mobile phones. Classroom based staff should store their mobile phones in a safe place away from the setting and should not access them in lesson and extra-curricular time. It is recommended that mobile phones are password protected and insured. Visitors, including contractors and parents/carers should be made aware of the NO USE policy on entry to the academy and through reminders such as posters and verbal reinforcement by members of staff accompanying them. Any photography required of the building (e.g., for estates/ICT purposes) should be completed when children are not present as far as possible and not published. Academy staff will challenge any use of mobile phones that does not adhere to this policy.

8.14 **Youth Produced Sexual Imagery:** this refers to youth produced sexual imagery, *nudes or pics* and includes both moving and still images. We will ensure pupils are taught in an age-appropriate manner the legal, social, and moral issues around sharing images such as these. Pupils will be encouraged to report all incidents. Teaching staff will inform the DSL who will act according to the ATT Safeguarding Policy and the guidance outlined in *Sharing nudes and Semi-Nudes: Advice for Education Settings Working with Children and Young People' (Gov.uk)*

8.15 **Radicalisation and Extremism:** the academy ensures pupils are safe from terrorist and extremist material when accessing the internet in school; this includes establishing appropriate levels of filtering. If a concern arises pupils will know who to go to and adults should inform the DSL who will act according to our *Safeguarding Policy* and the guidance

outlined in the Prevent Duty Guidance. The curriculum will ensure pupils are prepared positively for life in Modern Britain.

8.16 **Social Networking:** we are supportive of social networking on academy managed platforms as a tool to engage and collaborate with learners and to engage parents and the wider academy community within the tight principles set out in the staff code of conduct. Should staff wish to use other social media, permission must first be sought via the DSL who will conduct a risk assessment. The Principal will then be able to determine whether permission should be granted based on the findings of the risk assessment and other relevant information. **In addition, the following restrictions must be adhered to:**

8.17 Consent forms must be consulted before images or videos of any child are uploaded and no information shared which would contravene our *Data Protection Policy*

8.18 Where services are set to 'comment enabled' comments must be set to 'moderated'

8.19 All posted data must conform to copyright law; images, videos and other resources that are not originated by the academy are not allowed unless the owner's permission has been granted or there is a license which allows for such use.

8.20 **Notice and Take-Down Policy:** should it come to the Trust's attention that there is a resource which has been inadvertently uploaded and is inappropriate, or the academy does not have copyright permission to use that resource, it will be removed within one working day.

8.21 **Incidents:** any online safety incident is to be brought to the immediate attention of the DSL depending on the processes and procedures in place, or in their absence, the Principal. The DSL will assist you in taking the appropriate action to deal with the incident and fill out an incident log on CPOMS.

8.22 **Training and Curriculum:** Online safety for pupils is embedded into the curriculum and wherever ICT is used in the academy, staff will ensure that there are positive messages

about the safe use of technology and direction to protective factors and risks as part of the pupil's learning.

8.23 As well as the online safety sessions we will establish further training or lessons as necessary in response to any incidents.

8.24 The DSL is responsible for recommending a programme of training and awareness to the Principal and for consideration and planning.

8.25 Should any member of staff feel they have had inadequate or insufficient training generally or in any area this must be brought to the attention of the Principal for further CPD.

9. Educating Pupils with Online Safety

9.1 We will refer to and follow the DfE guidance:

- *Teaching Online Safety in Schools*
- *Relationships, Sex and Health Education*
- *Keeping Children Safe in Education*
- *Safeguarding Children and protecting professionals in early years settings: Online safety considerations*
- *Protecting children from radicalisation: The Prevent Duty*

9.2 Pupils will be taught about online safety risks. Online safety risks can be categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-

consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/)

9.3 We will regularly update pupils to make sure they are aware of the safe use of new technology both inside and outside of the academy.

9.4 Pupils will be taught about the importance of online safety and are encouraged to be critically aware of the content they access online, including extremist material and the validity of website content.

9.5 Pupils will be taught to acknowledge information they access online, to avoid copyright infringement and/or plagiarism.

9.6 Clear guidance on the rules of internet use will be present in all classrooms where ICT is used.

9.7 Pupils are instructed to report any suspicious use of the internet and digital devices to a member of staff.

9.8 Pupils will be made aware of online harms such as bullying, exploitation, radicalisation, grooming and online sexual harassment as well as protective factors and where to seek support.

9.9 We will embed learning about online safety through all relevant lessons and hold online safety events, such as *Safer Internet Day* and *Internet Day* and *Anti-Bullying Week*, to promote online safety.

10 Cyber Bullying and Online Sexual Harassment

10.1 This section must be reviewed alongside the *Anti-Child on Child Abuse and Bullying Policy* and the *Safeguarding and Child Protection Policy.* Cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images online.

10.2 Online sexual harassment (OSH) may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. It may include non-consensual sharing of sexual images and videos, sexualised online bullying, unwanted sexual comments and messages including those on social media, and sexual exploitation, coercion, and threats.

10.3 We recognise that both staff and pupils may experience cyber bullying or online sexual harassment (or other peer related online harms) and will commit to preventing and reducing online harms through clear policies, expectations and education.

10.4 We will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online. We strive to ensure a learning and

teaching environment which is free from harassment and bullying, for all staff and pupils, and any infringement of this should be reported to be the leadership of the academy in line with our Safeguarding, Anti-Child on Child Abuse and Bullying with Whistleblowing policies.

10.5 **In addition to the above guidance, we will refer to and follow the following guidance:**

- *Cyber Bullying: Advice for Head Teachers and Schools*
- *Preventing and Tackling Bullying: Advice for Head Teachers, staff and governing bodies*
- *When to call the police: guidance for schools and colleges*
- *Keeping Children Safe in Education*

11 Data and Cyber Security

11.1 Our Trust takes steps to protect the security of its computing resources, data, and user accounts. However, we cannot guarantee security. Staff, pupils, volunteers, parents, and others who use the ICT facilities should always use safe computing practices.

11.2 Our Trust Microsoft 365 platform will have multi factor authentication enabled for all staff accounts.

11.3 Login to our Microsoft 365 platform from outside of the United Kingdom has been blocked. This applies to both staff and pupils. We have a process in place that can temporarily allow international login, and a staff member can request this via the ICT Helpdesk.

11.4 Staff will be provided with a user account for accessing the ICT facilities, with their own username and password. This account will be tailored to the level of access they require and is for their individual use only.

11.5 Staff must not allow anyone to have access to their account under any circumstances, for any length of time, even if supervised.

11.6 The use of USB memory sticks and portable hard drives are strongly discouraged. More secure methods for transporting data are available via Microsoft 365 (SharePoint/OneDrive) or remote access functions. USB storage devices pose unnecessary risks around data breaches, viruses, and ICT security.

11.7 Staff must not use non-ICT-authorised third-party hosting services, like Dropbox, when processing data.

11.8 If staff use a personal computer at home for work purposes, they must ensure that any sensitive or personal information is secured to prohibit access by anyone who is not a member of the Trust's staff. The computer/device must also be encrypted.

11.9 All users (including staff, pupils, volunteers, and visitors) who bring a device not owned by the trust (Bring Your Own Device - BYOD) and wish to connect to the trust's network/Wi-Fi must ensure that the device is encrypted, has antivirus software installed, the operating

system and software are up-to-date and supported. Devices that do not meet these requirements will be denied access to the network until compliance is achieved.

11.10 Staff must ensure that portable computer equipment (such as laptops, tablets, mobile phones or digital cameras) are securely stored in a locked cupboard or room when left unattended. No equipment should be left unattended in a car, even if this is out of sight in the boot.

11.11 In the event of theft, loss or damage staff must contact the ICT Support team immediately.

11.12 Training and systems are put in place to minimise the risk of cyber security risks, phishing, or other email scams.

11.13 All users of our Trust ICT facilities should set strong passwords for their accounts and keep these passwords secure. Apart from early years and key stage 1, who will have account passwords set. Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

11.14 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.

11.15 All our Trust ICT devices that support software updates, security updates, anti-virus and monitoring products will be configured to perform such updates regularly or automatically.

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

11.17 All personal devices using the network must all be configured in this way.

11.18 All personal data must be processed and stored in line with data protection regulations and our *Data Protection Policy*.

11.19 All users of the ICT facilities will have clearly defined access rights to academy systems, files, and devices. These access rights are managed by the ICT Support team.

11.20 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 the ICT Support team immediately.

11.21 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 shut down completely at the end of each working day. Our Trust ensures that its devices and systems have an appropriate level of encryption.

11.22 Trust staff may only use personal devices (including computers and USB drives) to access data, work remotely, or take personal data (such as pupil information) off-site if they have been specifically authorised to do so by the senior leadership team.

11.23 Use of such personal devices will only be authorised if the devices have appropriate levels of anti-virus software, security and encryption, as defined by the ICT support team.

12 Internet Access

12.1 Our Trust has Wi-Fi/wireless networks that will provide access to the internet; these are secured and have the appropriate level of filtering. The academy may have separate Wi-Fi/wireless networks such as ATT WIFI, Domain (academy devices connected to the network), BYOD (bring your own device) and Guest network. Details about the networks available and how to access is available from the ICT Support team.

12.2 Pupils will only be able to use the Wi-Fi/wireless networks that have already been setup for the domain devices (academy devices connected to the network) unless a BYOD network is available.

12.3 Members of staff or pupils must not to connect to any Wi-Fi network that is not secure (secure networks show a padlock symbol next to the network name) or use an internet/cybercafé to access our Trust ICT facilities.

12.4 Parents and visitors to the academy will not be permitted to use the Wi-Fi/wireless networks unless specific authorisation is granted by the Principal, ICT support team, or there is a Guest network available. Authorisation will only be granted if:

- Parents are working with the academy in an official capacity (e.g., as a volunteer or as a member of the PTA)
- Visitors need to access the academy's Wi-Fi to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan).

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

13 Social Media

13.1 Social media sites have become important learning, communication, and marketing tools as they allow users (individual, academy, or Trust) to interact and raise their profile with a wide cross section of other users. *Social networking* is defined as sharing your interests and thoughts in an online forum with like-minded individuals. *Social media* is how this is completed.

13.2 Our Trust and academies have an official social media page(s). Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

13.3 Social media should never be used in a way that breaches any Trust policy.

13.4 We have guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they always abide by these guidelines.

13.5 Staff members, Trustees and Governors must be conscious at all times of the need to keep their personal and professional lives separate. They should not put themselves in a position where there is a conflict between their work for the Trust and their personal interests.

13.6 Staff members, Trustees and Governors must be cautious of what content they share and should not engage in any political content.

13.7 Staff members, Trustees and Governors must not engage in activities involving social media which might bring our Trust into disrepute.

Staff members, Trustees and Govervors must not represent their personal views as those of our Trust, on any social medium. If they express any idea or opinion, they should add the disclaimer such as 'these are my own personal views and not those of the academy/Trust'.

13.8 Staff members must not discuss personal information about pupils, our Trust staff, and other professionals they interact with as part of their job on social media. They must not divulge any information that is confidential about our Trust or partner organisations

13.9 Staff members, Trustees and Governors must not use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations, or our Trust.

13.10 The ATT logo, academy logo or intellectual property may not be used in connection with any blogging or social networking activity without permission from the Principal/Trust.

13.11 No post should cause others embarrassment or harm.

13.12 Staff members, Trustees and Governors must not knowingly have contact through personal social media with any pupil across our Trust unless the pupils are family members.

13.13 Staff members, Trustees and Governors should ensure that they adopt suitably high security settings on any personal profiles they may have.

13.14 Staff members, Trustees and Governors must exercise caution in their use of all social media or any other web-based presence that they may have, including written content, videos or photographs, and views expressed either directly or by liking, sharing certain pages or posts established by others. This may also include the use of dating websites where employees could encounter pupils either with their own profile or acting covertly.

13.15 Staff members, Trustees and Governors must not have any contact with pupils' family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.

13.16 If staff members, Trustees or Governors wish to communicate with pupils through social media sites or to enable pupils to keep in touch with one another, they can only do so with the approval of our Trust (where applicable) and through official sites created.

13.17 Staff members, Trustees and Governors must not allow anyone they can identify as a pupil to follow them or accept friend requests. If any such requests from pupils who are not family members, are received they must discuss this with our Trust or academy Designated Safeguarding Lead. They can be directed to follow our Trust/academy social media accounts.

13.18 On leaving our Trust, staff members must not contact pupils/former pupils by means of personal social media sites.

13.19 Photographs, videos, or any other types of digital images depicting pupils wearing uniforms or clothing with academy logos or images identifying academy premises must not be published on staff members' personal web space or personal social media sites

14 Use of Artificial Intelligence (AI) – Safe and Responsible Practice

The Trust recognises the growing use and educational potential of Artificial Intelligence (AI) tools. To ensure these technologies are used responsibly, ethically, and safely by both staff and pupils, the following must apply.

General Principles

14.1 AI tools may only be used to enhance teaching, learning, or administrative efficiency, and not to replace professional judgement or critical thinking.

14.2 All AI use must comply with data protection, safeguarding and other existing policies.

14.3 Staff and pupils must not use AI to generate or share content that is inappropriate, offensive, discriminatory, or misleading.

Staff Use of AI

14.4 Staff may use AI to support lesson planning, resource creation, and workload management, but must verify the accuracy and appropriateness of any AI-generated content.

14.5 Personal or confidential data (e.g., pupil names, health records, assessments) must never be entered into AI platforms unless specifically approved by the Academy's data protection lead.

14.6 Staff must remain accountable for any work produced or assisted by AI and should not rely on AI to make decisions related to pupil assessment, behaviour management, or safeguarding.

14.7 Staff must only use approved AI platforms that meet the organisation's cybersecurity standards.

14.8 When using AI in the classroom, staff should ensure students understand its limitations and ethical implications.

14.9 If staff require Microsoft Teams meetings to be recorded or transcribed, they must use the tools that are part of Microsoft Teams. No other 3rd party AI tools, such as AI note takers are allowed. This is in line with GDPR compliance and how AI products use our data.

Pupil Use of AI

14.10 Pupils may use AI tools under supervision or as directed by staff, where appropriate, for learning, exploration, or creativity.

14.11 Pupils must not use AI to complete assessments, coursework, or homework in a way that misrepresents their own understanding or abilities (e.g., plagiarism).

14.12 Pupils must be taught to critically evaluate AI-generated content, understanding that it may contain inaccuracies or bias.

14.13 Misuse of AI tools (e.g., generating harmful, misleading, or offensive content) will be treated as a breach of the Behaviour Policy or other policies and procedures.

Monitoring and Review

14.14 The Trust will regularly review its guidance on AI use in response to technological developments and updates in DfE guidance.

14.15 Training and support will be provided to staff to ensure they are confident in using AI tools safely and appropriately.

Formal Assessments

14.16 Staff must take reasonable steps to prevent malpractice involving generative AI in assessments.

14.17 Staff must follow guidance from the Joint Council for Qualifications on AI use in assessments.

14.18 Staff and exam centres must understand what constitutes AI misuse and how to detect and prevent it.

14.19 AI must not be used in a way that compromises the integrity of marking or assessment outcomes.

Intellectual Property

14.20 Staff and pupils should be aware of intellectual property (IP) implications when using generative AI tools.

14.21 Copyrighted materials must not be used to train AI unless permission is granted or a legal exception applies.

14.22 Work created by pupils and staff should be treated as copyright material.

14.23 Copyright law must be considered separately from data protection law. Consent for personal data use does not cover copyright compliance.

14.24 Users should be cautious when using free AI tools, as our data may be used to train models. Paid tools may offer opt-out options. Staff can contact the ICT Support team if they are unsure.

14.25 Examples of copyrightable content include:

- Essays, homework, or drawings by pupils
- Lesson plans by teachers
- Prompts entered into AI tools

- Data Privacy

14.26 It is important to be aware of the data privacy implications when using generative AI tools.

14.27 Personal data must be protected in accordance with data protection legislation. Personal data must not be used in generative AI tools.

14.28 If it is strictly necessary to use personal data in generative AI tools within a setting, the staff must ensure that all steps are taken to protect the data, and the products and procedures comply with data protection legislation and GDPR.

Appendix 1 – Acceptable Use Agreement (Staff and Volunteers)

Background

Technology has transformed learning, entertainment, and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should always have an entitlement to safe internet access. Within ATT, online safety is the responsibility of everyone. As such all staff and volunteers should promote positive safety messages in all uses of ICT whether with other members of staff or with pupils.

This Acceptable Use Agreement is intended to ensure that:

- Staff and volunteers will act responsibly to stay safe while online, being a good role model for younger users
- Effective processes and procedures are in place for the online safety of all users and the security of devices, systems, images, personal devices, and data
- Staff and volunteers are aware of, and can protect themselves from, potential risk in their use of online technologies
- Staff and volunteers are using AI responsibility and are aware of the risks
- This should be read in conjunction with the ATT Staff Code of Conduct

For my professional and personal safety, I understand that:

- I will ensure that my online activity, including the use of social networking sites does not compromise my professional responsibilities, nor bring the Trust or academy into disrepute.
- My use of technology, including the internet and software, will be monitored through academy systems.
- I will not use technology provided by the Trust for personal business (including emails) unless permission has been given by the Principal/Director.

Communication

- When communicating professionally, I will use technology provided by the Trust e.g., not using personal email addresses, mobile phones, (unless checked and agreed by the DSL) or social media logins for work related communications.
- I am aware that academy data, including emails, is subject to the ATT Freedom of Information Policy and will therefore ensure that all communications are kept professional.
- I will ensure that all communications on behalf of ATT or the academy to external organisations are professional and where I am unsure of suitability of content, I will seek advice from my line manager. I understand that I am responsible for the content that I send.
- I will not use my personal mobile phone when in a classroom environment or when with or supervising pupils. I will store my mobile phone safely away from pupils' access.

The Network

- I will not disclose my login username and password to anyone. I understand that there is no occasion when a password needs to be shared with another member of staff, pupils, or ICT Support.
- I will change my password regularly.
- I will not allow pupils or colleagues to use my network/computer user account to access any ICT facilities (e.g., MIS). I understand that if I do allow pupils or colleagues access it could lead to a breach of the *Data Protection Policy* and network security.
- I will log off the network or lock my computer and check that the logging off procedure is complete before leaving my computer.
- I will be vigilant when clicking email/web links to ensure they are safe as this could cause a cyber breach. If unsure, discuss with ICT Support.

For the safety of others

- I will not copy, remove, or otherwise alter any other user's files, without authorisation
- I will share the personal data of others only with their permission.

Images and Videos

- I will not upload onto the internet site or service images or videos of other staff or pupils without consent. This is applicable professionally (in the academy) and personally (e.g., staff outings).
- I will not take or store images and videos of pupils on a personal device.

Virus and other Malware

- I will report any phishing email/virus outbreak/cyber-attack to ICT Support as soon as possible, along with the details and the actions taken.

For the safety of all

- I will not deliberately bypass any systems designed to keep everyone safe.

Internet access

- I will not intentionally access or attempt to access anything illegal, harmful, or inappropriate, including child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting radicalisation and extremism; promoting illegal acts; and any other information that maybe offensive to colleagues.
- It is my responsibility to immediately report any illegal, harmful, or inappropriate incident to the DSL or Principal/Director.

Social Networking

- I will not share my online personal information (e.g., social networking profiles) with the children and young people in my care. Staff using social networking for personal use should never undermine the academy (e.g., its staff, parents and/or pupils). Inappropriate use of social media during and outside of work hours could lead to disciplinary action.
- Social networking is allowed in the academy when the site is managed through the academy. Personal use is not allowed.
- I will not become 'friends' with academy parents or pupils on social networks, unless a pre-existing relationship exists (e.g., niece, nephew etc.). If this applies, I must disclose such relationships to line managers or DSLs to ensure safeguarding oversight.

Data Protection

- I will only transport, hold, disclose, or share personal information about myself and others, as outlined in our *Data Protection Policy*. Where personal data is transferred externally, it must be encrypted or securely shared.
- I understand that the *Data Protection Policy* requires that any personal data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by the *Data Protection Policy* to disclose such information to an appropriate authority.
- If it is necessary for me to take work home, or ICT equipment (laptop, USB, pen drive etc.) offsite, I will ensure that it is encrypted, or the data is kept securely. Before doing this, I will ask ICT Support to confirm it is encrypted. I understand that under no circumstances should data concerning personal information be taken offsite on an unencrypted device. No equipment or paperwork should be left unattended in a car, even if this is out of sight in the boot.

I confirm that:

- I have read and agree to abide by the *Acceptable Use Agreement (Staff and Volunteers).*
- I have read and understand our *ICT Policy*, the *Staff Code of Conduct* and Whistleblowing and Safeguarding policies.
- I understand that breaches of the *Acceptable Use Agreement (Staff and Volunteers)* are subject to disciplinary action under the *Disciplinary Procedure*.

If you are unsure about responding to any of the above statements, please contact the Principal or Director of ICT.

Name: _____

Role/Job Title: _____

Signature: _____

Date: _____

Appendix 2 - Acceptable Use Agreement for Pupils

(KS2 and above)

Technology is a part of learning, entertainment, and communication however the use of technology can also bring risks. It is important that you learn to recognise risks and take action to stay safe. When using technology within the academy, you must agree to the following:

- **I understand** that my use of academy owned technology systems and devices is monitored when I am working both on and offline (including email and internet searches) and this includes devices given to pupils to use at home.
- **I will** be respectful to everybody online. I will treat everybody the way that I want to be treated.
- **I will** use AI responsibly
- **I will** be polite and responsible when I communicate with others.
- **I will not** share personal information online with anyone and understand why this is dangerous.
- **I will** let my teacher or responsible adult in school know if anybody asks me for personal information.
- **I understand** that some people on the internet are not who they say they are and that some people may be unkind and wish me harm. I will tell my teacher if I am ever concerned in the academy or my parents if I am at home.
- **I will** let my teacher or responsible adult in school know if someone has accessed or shared a website, image or information that is offensive or illegal.
- **I will** let my teacher or responsible adult in school know if anybody says or does anything to me that is hurtful or upsets me.
- **I promise** to only use the academy ICT for schoolwork that the teacher or responsible adult in school has asked me to do.
- **I promise** not to look for or show other people things that may be offensive or distressing.
- **I promise** to show respect for the work that other people have done.
- **I will not** use other people's work or pictures without permission to do so.
- **I will not** damage the ICT equipment. If I accidentally damage something I will tell my teacher.
- **I will not** share my password with anybody. If I forget my password, I will let my teacher know.
- **I will not** use other people's usernames or passwords.
- **I will not** download anything from the internet unless my teacher has asked me to.
- **I will not** try to access anything illegal.
- **I will not** sign up to and use social networking sites I am not permitted to.
- **I will not** access or share any sites or information that may cause offence or harm to me or others.
- **I will** only use my personal device if I have received permission from a member of staff.
- **I understand** that I am responsible for my actions and the consequences. If I break the rules in the Acceptable Use Agreement, there will be consequences of my actions, and my parents will be told.

Mobile devices

- I will only use personal mobile devices during out-of-school hours in accordance with the ICT Policy and my own academy's rules

- I will ensure that my mobile device is either switched off or set to silent mode during school hours and will only use my device to make or receive calls when an adult permits me to do so.

- I will seek permission/consent before a device is used to take images or recordings.
- I will not use any mobile devices to take pictures of fellow pupils or adults unless I have their consent.
- I will not take or store images or videos of staff members on any mobile device.
- I will not use any mobile devices to send inappropriate messages, images, or recordings.
- I will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.
- I will not access the Wi-Fi system using personal mobile devices, unless permission has been given by the Principal.

I have read and understood the above and agree to follow these guidelines.

Name of Pupil: _____

Signed: _____

Year Group: _____

Date: _____

I have read this *Acceptable Use Agreement* and understand that my child's internet access could be monitored to ensure that there is no illegal or inappropriate activity by any user of the academy network. I acknowledge that this has been explained to my child and that they have had the opportunity to voice their opinion and to ask questions.

Name of Parent: _____

Signed: _____

Date: _____

Appendix 3 - Acceptable Use Agreement for Pupils (KS1 and Under)

Adult assistance must be given when required for full understanding.

Technology is a part of learning, entertainment, and communication however the use of technology can also bring risks.

It is important that all children learn to recognise risks and take action to stay safe. When using technology within the academy, they must agree to the following rules:

I will ask an adult if I want to use the computer.

I will tell an adult if I see something that upsets me on the screen.

I will only go to activities that an adult has told or allowed me to use.

I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.

I know that if I break the rules, I might not be allowed to use the computer.

I know that my use of computers is checked to make sure that I am being safe.

If I have a mobile phone that I bring to school – **I will** abide by my academy's rules about mobile phones and other devices.

I agree to follow the rules for using a computer.

Name of Pupil: _____

Signed: _____

Date: _____

I acknowledge that the rules have been explained to my child and that they have had the opportunity to voice their opinion and to ask questions.

I understand that academy equipment is monitored when lent to a pupil to use at home as well as in the academy.

Name of Parent/Carer: _____

Signed: _____

Date: _____