E-Safety Policy

Academy Transformation Trust

Review Date

February 2023

Ratified

30 March 2023

Next Review

March 2026

Responsible Directorate

Safeguarding and Operations

Our Vision

Transforming Lives of our learners

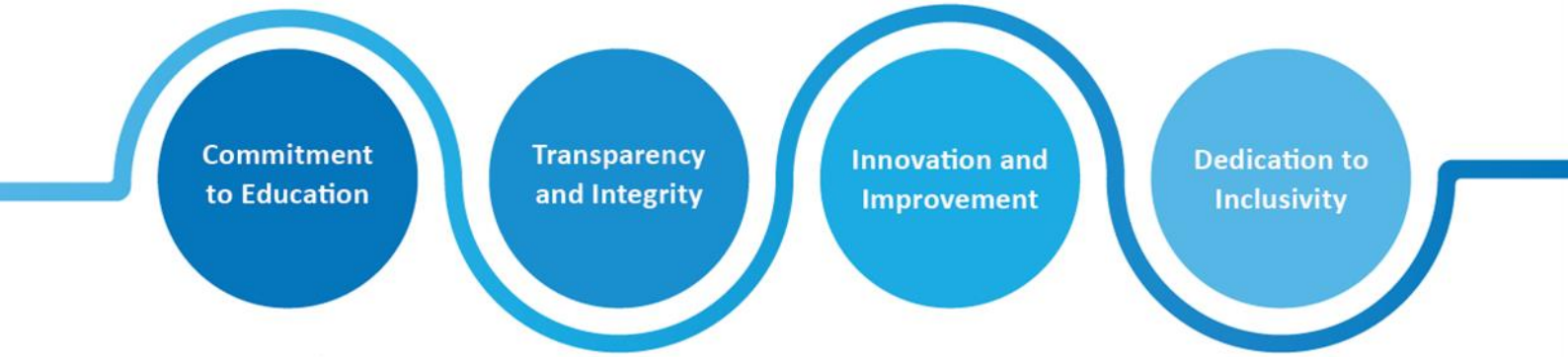
We seek to ensure that all our learners receive a high-quality education from expert staff and aspire to achieve the best they possibly can, no matter their background or ability. Our learners have safe, supportive learning environments in which they develop, grow, and challenge themselves. We are determined that our learners will receive the very best enrichment and opportunities to help them reach their full potential and ensure they are prepared for the future, wherever it might take them.

Transforming Lives of our colleagues

Our colleagues are supported with the very best professional development through our innovative ATT institute, allowing them to stay focused on learning and developing as practitioners whilst they progress in their careers. We share the very best practice across our community of academies to help build systems and processes that really work.

Transforming Lives in the communities we serve

We are committed to actively engaging with and addressing inequality in our local areas. We understand that every one of our academies and their diverse communities are different, so we aim to build a supportive, collaborative, and nurturing relationship with each whilst sharing our key values across our Trust.



Our Values

Commitment to Education

Our core purpose is to positively impact the lives of all our learners. Education will always be at the heart of everything we do.

Transparency and Integrity

We are proud of our success whilst being open and honest about our areas for improvement. Our actions are always ethical and in the best interests of all our stakeholders.

Innovation and Improvement

We are committed to innovative education- always moving forward and never standing still. Our learners are ambitious and prepared for a future that is constantly changing and developing.

Dedication to Inclusivity

Our learners are all different and all important to us. We aspire to support, challenge, and help each one of them reach their full potential, regardless of their background or level of ability.

Contents

Statement of Intent

Academy Transformation Trust (ATT) is committed to safeguarding children and young people, and we expect everyone who works within ATT to share this commitment. This policy sets out how our academies will deliver these responsibilities specifically related to online harms, behaviours, and responsibilities.

Our academy uses technology extensively across all areas of the curriculum. Online safeguarding (e-safety) is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, or a change in statutory guidance, whichever is sooner.

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 e-safety training annually.

We provide a specially designed 'safer schools' app for all of our pupils, staff, parents and governors. The app offers credible information about online safety of how to deal with online harms (even when the academy is closed) training, resources, quizzes, and a frequent tiny push alerts to keep adults aware of the latest online trends, challenges, and apps along with the associated risks and safety features. It also supports parents to talk to their child in an age-appropriate way about the online harms that they must safeguard against or anything that is worrying their child.

Please ensure that you have downloaded the **free** *Safer Schools* app details of which are available from your DSL or DDSL.

1 | Safeguarding Roles and Responsibilities

1.1 The Designated Safeguarding Lead (DSL) is a member of the academy senior leadership team and holds the strategic oversight to ensure that safeguarding, including E-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.

1.2 The **Local Governing Board** will:

1.2.1 Maintain their statutory responsibility for monitoring the academy's approach to e-safety as part of their overall safeguarding duties.

1.2.2 The Governor with responsibility for safeguarding should include the governance of e-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 e-safety training within the academy
- Recommend further initiatives for e-safety training and awareness within the academy.

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

1.3 The **Principal** will:

- Have overall responsibility for e-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 e-safety requirements within this policy.
- Delegate the responsibility for the technical elements of e-safety to a member of ICT Support staff. The member of staff with responsibility for the technical elements of e-safety will be known as ICT Support for the purposes of this policy.
- Ensure e-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 e-safety training is arranged for all staff, in line with core safeguarding training, and that new guidance is shared.
- Ensure that all e-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 e-safety is appropriately addressed for all pupils through the curriculum.
- Ensure that parents and carers are told what filtering and monitoring systems we use, so they can understand how the academy works to keep children safe. This is set out in *Section 4* below.

- 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.

1.4 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 e-safety matters.
- Engage with parents and the academy community on e-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 e-safety incidents; ensure staff know what to do if an incident is reported by Smoothwall and ensure an effective response and appropriate audit trail.
- Ensure technical e-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 e-safety training as part of their annual core safeguarding training. Colleagues will also receive updates throughout the year from the DSL and through the Safer Schools app.
- If the E-Safety Officer is **not** the DSL, appropriate communication should be identified to ensure correct safeguarding procedures are in place.

1.5 **ICT Support** will:

1.5.1 Be responsible for ensuring that the ICT technical infrastructure is secure and monitored; this will include ensuring the following:

- Anti-virus is fit-for-purpose, up to date and applied to all capable devices
- Operating system updates are regularly monitored, and devices updated as appropriate
- Any e-safety technical solution such as internet filtering or monitoring are operating correctly
- 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
- 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.
- 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
- To always operate with integrity and never abuse the position of trust that administrators are placed in.

1.6 **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 e-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 e-safety incident is reported to the DSL via CPOMS or the Principal if the matter is adult related.
- Promoting and sharing e-safety practices are planned for and embedded into the curriculum.

1.7 **Pupils** will:

- Understand the boundaries for the use of Academy Transformation Trust ICT equipment and services. **These are given in the Pupil Acceptable Use Policy 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 Smoothwall, and concerns shared with the safeguarding team or Principal.
- Understand that e-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.

1.8 **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 Smoothwall 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 *Pupil Acceptable Use Agreement*.
- Support the academy when sanctioning pupils for compromising the e-safety of themselves or others.

2 | The Acceptable Use Agreement

2.1 All new colleagues and volunteers will sign the *Acceptable Use Agreement* (Appendix 1) as part of their induction.

2.2 Upon signing the Acceptable Use Agreement, staff and volunteers will be permitted access to academy technology including the internet. In signing the Staff and Volunteers Acceptable Use Agreement or record sheet, staff and volunteers are also signing to confirm that they have read and understood the ATT *E-Safety Policy*.

2.3 All pupils and parents will sign a copy of the appropriate **Pupil Acceptable Use Agreement** (Appendices 2 & 3 depending on age) when they join the academy. Once this is in place pupils will receive an annual update and reminder as part of the welcome back activities each September. This could also be discussed in parent/academy meetings on entry to ATT academies or at transition points.

2.4 All pupils will be guided through the policy and the acceptable use of ICT by an ATT colleague to ensure they understand the risks associated with online behaviours and harms and the protective factors that are in place for the and appropriate use to ensure that they are able to make the right choices when using IT and/or working online.

3 | Unacceptable Use

3.1 The following is considered unacceptable use of our ICT facilities by any member of the academy community. Any breach of this policy may result in disciplinary or behaviour proceedings. Unacceptable use of the 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
- 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
- Sharing passwords and/or logging in to the ICT facilities with a user account not assigned to you
- 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 academy's filtering mechanisms

3.2 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 | Technology

4.1 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:

4.2 **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 required (this may be through third party support).

4.3 **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.

4.4 **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.

4.5 **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.

4.6 **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 who will act accordingly.

4.7 **Passwords: s**taff 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.

4.8 **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.

4.9 **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*.

4.10 **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 ICT Support if unsure.

4.11 **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.

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

4.13 **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.

4.14 **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)

4.15 **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.

4.16 **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:**

- 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*
- Where services are set to 'comment enabled', comments must be set to 'moderated'
- 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.

4.17 **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.

4.18 **Incidents:** any e-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.

4.19 **Training and Curriculum:** E-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.

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

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

4.22 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.

5 | Educating Pupils

5.1 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*

5.2 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 such as pornography, fake news, misogyny, self-harm, suicide, radicalisation and extremism
- **Contact:** being subjected to harmful online interaction with other users such as peer to peer pressure and adults posing as children or young adults to groom or exploit children
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm such as making, sending and receiving explicit images, sharing other explicit images and online bullying
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing or financial scams.

5.3 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.

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

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

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

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

5.8 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.

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

6 | Cyber Bullying and Online Sexual Harassment

6.1 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.

6.2 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.

6.3 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.

6.4 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 the leadership of the academy in line with our Safeguarding, Anti-Child on Child Abuse and Bullying and Whistleblowing policies.

6.5 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*

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, e-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 Policy 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.
- 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 academy for personal business (including emails) unless permission has been given by the Principal
- I will not use personal ICT equipment for professional purposes unless a risk assessment has been carried out by the E-Safety Officer and the E-Safety Officer has granted permission and use is therefore agreed.

Communication

- When communicating professionally, I will use technology provided by the academy e.g., not using personal email addresses, mobile phones, (unless checked and agreed by the E-Safety Officer, see above) 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.

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.).

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.

I confirm that:

- I have read and agree to abide by the *Staff and Volunteers Acceptable Use Agreement.*
- I have read and understand our *E-safety and ICT Policy*, the *Staff Code of Conduct* and Whistleblowing and Safeguarding policies.
- I understand that breaches of the *Staff and Volunteers Acceptable Use Agreement* 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** 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 *E-Safety 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 been offered the Safer Schools app for any personal devices for free and understand why it is valuable in keeping me safe (Page 3 of the *E-safety Policy*).

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 Policy* 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 (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 am aware of the Safer School app (page 3 of the E-safety Policy) and that there are different version that I can have (parent or child) so that I can access the information with my child about staying safe online and that I can download the children's version on any device that my child has access to.

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: _____

Appendix 4- 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 academy to use the ICT facilities, including governors, staff, pupils, volunteers, contractors, and visitors
- **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
- **Personal use:** any use or activity not directly related to the users' employment, study, or purpose
- **Authorised personnel:** employees authorised by the academy/our 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