GREAT HEIGHTS ACADEMY TRUST

Achieving excellence together

Acceptable Use of Digital Technologies Policy

Approved by:	Trust Board		
Responsible department:	Core MAT Team		
Last review date:	June 2025	**Last reviewed by:**	IT Manager – Adam Hutchinson
Last updated:	June 2025	**Last updated by:**	IT Manager - Adam Hutchinson
Next review due:	June 2026		

1. What is a 'Use of Digital Technologies Policy'?

This policy sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all digital/online technologies within the Trust.

2. Why have a 'Use of Digital Technologies Policy'?

The use of digital/online technologies has become an integral part of Trust life. It is imperative that there are clear rules, procedures and guidelines to minimise inherent risks.

These risks include:

- Security issues including the ever-evolving threats of viral/cyber attacks
- Potentially illegal activities such as downloading copyright materials/file-sharing and more serious issues such as cyber-bullying, the creation and sharing of sexual imagery and grooming
- Exposure or access to extremist or terrorist materials. Radicalisation.

It is important that all staff are clear about appropriate procedures to protect the Trust, all its members and themselves.

The Trust acknowledges that whilst it will endeavour to safeguard against all risks it may never be able to completely eliminate them. Any incidents that may arise will be dealt with quickly and according to policy to ensure that all members of the Trust community are best protected.

3. Policy Aims

- To ensure the safeguarding of all pupils within and beyond academy settings
- To protect all Trust staff within and beyond Trust settings
- To protect the Trust from any negative impacts caused by harm or threat to any of its uses of digital technologies, whether these be of accidental or malicious cause
- To have clarity about Trust procedures and the roles and responsibilities of all in it

4. Roles and Responsibilities within a Trust Academy:

4.1 Roles: Trust Boards, Principals and Vice-Principals

It is the overall responsibility of the Principal and Vice-Principals with an LGB to ensure that e-Safety and Digital Security are well-managed in each Academy:

- The Principal and Vice-Principals are responsible for promoting e-Safety and Digital Security throughout an academy and have an awareness of how this is being developed
- They will implement agreed policies, procedures and staff-training, taking the lead responsibility for ensuring e-Safety and Digital Security are addressed in order to establish a safe learning/working environment.
- The Principal will inform the LGB about the delivery of the e-Safety curriculum, ensuring that the LGB know how this relates to child protection.
- The Principal will inform the LGB about the promotion and maintenance of Digital Security.
- The LGB must ensure Child Protection is covered with an awareness of e-Safety and be clear how it is being addressed within each Academy. It is the responsibility of the LGB to ensure that all Child Protection guidance and practices are embedded.
- These parties will jointly ensure that any misuse or incident is dealt with according to policy and appropriate action is taken, to extremes such as suspending a member of staff, excluding a pupil or involving the Police. See appendices for procedures on misuse.

4.2 Roles: Trust IT Director and Academy e-Safety/Digital Security Leaders

It is the role of the Trust IT Director with designated e-Safety/Digital Security Leaders to:

- Liaise with the PSHE, Child Protection and Computing/ICT leads so that all policies and procedures are up to date to take account of any emerging issues and technologies.
- Provide up-to-date information for all staff to teach and manage e-Safety effectively.
- Involve parents/carers so they feel informed and know where to go for advice.
- Ensure there is appropriate and up-to-date anti-virus and anti-spyware software on all susceptible devices and that this is reviewed and updated on a regular basis.
- Ensure that filtering is set to the correct level for staff and pupils at the initial set up of all devices and within any online environments.
- Develop and maintain staff awareness of the nature and likelihood of phishing and cyber-attacks. Train staff to be alert to the typical signs of such attacks and to know how to best protect themselves, the Academies and the wider Trust from these.
- Have an overview of all Academy digital/online technology usage - it is a teacher's responsibility to monitor such usage by the pupils in their care.
- Keep a log of incidents for analysis to help inform future development and safeguarding.
- Report issues and update the Principal on a regular basis.
- Setup accounts for all academies' students and staff adhering to standard approved naming structures.
- Install and monitor IT Security solutions such as Anti-Virus and NAC Software to monitor networks and devices.
- Configure security software to disallow removable media to prevent the transfer of viruses to a Trust network.

4.3 Roles: All Staff/Adults in an Academy

It is the responsibility of all staff/adults within an Academy to:

- Ensure that they know who the Designated Person for Child Protection is so that incidents which involve a pupil can be reported. Where an allegation is made against a member of staff it should be reported immediately to the Principal. In the event of an allegation made against the Principal, the Chair of Governors must be informed immediately.
- Report incidents of cyber-bullying or other inappropriate behaviour via digital technologies in the same way as for other non-physical assaults.
- Be up to date with e-Safety knowledge that is appropriate for the age group they work with and embed this throughout the curriculum.
- Ensure that all pupils are protected and supported in their use of online technologies so that they know how to use them in a safe and responsible manner and know what to do in the event of an incident.
- Respond promptly if a pupil believes any of their passwords is known by others.
- Only upload pupil information, as required by specific job roles, to online database-requiring services (for example Seesaw and Arbor) for agreed purposes*, such as monitoring pupil progress and/or enhancing their learning. *Such service providers must have been approved by the school and vetted by the Trust Data Protection Officer.
- Alert the e-Safety/Digital Security Leader of any new or arising issues and risks that may need to be included within policies and procedures.

4.4 Roles: All Staff/Adults in the Trust

It is the responsibility of all staff/adults within the Trust to:

- Be aware of the Prevent (Radicalisation) Agenda and act appropriately upon any concerns.

- Keep Academy/Trust information confidential and not breach the Data Protection Act.
- Not disclose security passwords or leave a device unattended when they are logged in.
- Follow security procedures if any data is required to be taken from Trust premises.
- Be alert to the signs of phishing/cyber-attacks, e.g., anything unexpected about the arrival, nature or layout of an email, especially if it invites the recipient to click on a button, follow a link or open an attachment. Such emails should be deleted or further enquiries made.
- Report any accidental 'misuse' or access to inappropriate materials to a senior line manager.
- Appropriately use only devices provided by (or authorised by) an Academy/the Trust. Any use deemed necessary of personal equipment, should be agreed with, or reported promptly to a senior line manager & IT Team.
- Only use Academy/Trust provided USB memory sticks with approval from the IT Team and follow agreed encryption procedures.
- Use devices provided by the Academy/Trust when working at home/remotely or ensure that any personal devices used for work purposes at home have up-to-date anti-virus and malware protection and are password protected.
- Sign an Agreed Usage Statement to confirm that they agree with and accept the rules for staff/adults – see Appendix 2.

4.5 Roles: Academy Pupils

Pupils will be:

- Taught to use digital/online technologies in a safe and responsible manner through Computing/ICT, PSHE and across the curriculum.
- Taught to tell a trusted adult about any concerns they have re. their use of digital technologies (including contacts from someone they do not know) or any other issues causing upset straightaway.

As pupils get older, they will increasingly:

- Take responsibility for their own and each other's safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school
- Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.
- Ensure that they are choosing secure passwords and not sharing these with other pupils.

Primary age pupils will be taught about and asked to follow age-appropriate guidance which will be displayed in their classrooms – see appendices 3a and 3b.

Secondary age pupils must sign an Agreed Usage Statement to confirm that they agree with and accept the Trust Digital Technology usage requirements – see Appendix 4.

4.6 Roles: Academy Parents/Carers

The Trust wants parents/carers to feel involved and active in the e-safety education of their children. Academies should keep parents informed about potential risks and current best guidance. Parents should know where to go for advice and support, starting with their child's class teacher. It should be clear that this support extends beyond the school day and gates; it is more likely that issues will occur outside of schools rather than within.

Parents can communicate with the Academy staff via their academy/trust email addresses following clear protocols and rules. All such communications must be:

- Polite and related to school matters only
- Only sent between 8am and 6pm on days when a school is open to pupils*

*Outside of these times parents should use the main school admin/contact email address.

There are systems in place for storing all electronic communications which take place between school and parents. These can be monitored and checked as required.

If these rules by a parent, the parent may be required to make all future communications through the main school admin/contact email address.

5. Appropriate Use by Trust Staff/Adults

Staff members who have password protected access to the Trust/Academy networks have this so that they can access, develop and manage appropriate resources for their work within the Trust. Staff also have access to a range of peripheral ICT equipment which is similarly resourced/supplied to appropriately deliver the work of the Trust/its Academies.

All staff will be made aware and asked to read/follow this Policy, including Appendix 1: 'Trust-wide Digital Security' and then be required to sign the 'Agreed Usage Rules' for Staff (appendix 2a); these make clear how the Trust's digital/online resources should be used. An abridged version of the Rules will be given to adults who visit/work in a Trust setting for a short time (appendix 2b).

Staff will not be given logins for Academy/Trust networks until they have signed the relevant AUP.

5.1 In the event of Inappropriate Use by Trust Staff/Adults

If a Trust employee is believed to have deliberately misused any of the Trust's digital/online resources in any manner felt to be inappropriate, a report must be made to the staff member's Principal or Senior Manager immediately. Also see Appendix 5a – 'Procedures Following Misuse by Staff' (this includes minor events and accidental misuse and has for a list of actions relating to the scale of the incident).

6. Appropriate Use by Academy Pupils

Within the Trust pupils are taught to use the digital/online technologies in a safe and responsible manner, for example, knowing how to conduct research or write a message to another pupil. The downloading of content, for example music files or photographs needs to be appropriate and 'fit for purpose' e.g., based on research for work and be copyright free. Pupils will be taught about the implications of misusing digital/online technologies e.g., posting hurtful/inappropriate material online.

In the event that a pupil accidentally accesses upsetting or inappropriate content the pupil should know appropriate actions to take e.g., close the window and report this to a member of staff immediately.

Where a pupil feels unable to disclose any issues or misuses against them to a trusted adult, they should have been made aware of the facilities such as the CEOP Report Abuse button (www.thinkuknow.co.uk) and Childline number (0800 1111) to seek advice and help.

6.1 In the event of Inappropriate Use by Academy Pupils – 'Internal'

Pupils will be supported if there are any accidental incidents. Should a pupil be found to have deliberately misused digital/online resources the following consequences will occur:

- The parents/carers of the pupil will be contacted
- A formal incident record will be made
- Further or serious misuse of the rules may result in a suspension of access to some or all digital/online resources for a period of time and a letter will be sent to

parents/carers (this would include any incident where a pupil is deemed to have misused technology against another pupil or adult).
- Depending on the seriousness of the incident other sanctions may be employed.

Also see Appendix 5b – 'Procedures Following Pupil Misuse or Incident'

6.2 In the event of Inappropriate Use by Academy Pupils – 'External'

If the Academy becomes aware of an incident outside of school, it will raise this with any parents/carers involved and offer guidance toward its resolution. In extreme cases some such situations may require the contacting of outside agencies such as the police, or in cases of radicalisation to the Channel Scheme.

In cases of 'youth produced sexual imagery', (a specific definition of 'sexting') an Academy will follow 'Sexting in schools and colleges: Responding to incidents and safeguarding young people'.

All members of staff (including non-teaching) will be trained how to recognise and disclose such incidents and pupils will be given age-appropriate e-Safety teaching in this area.

6.3 In the event of concerns of Radicalisation within the Trust

In respect of safeguarding individuals from radicalisation, the Trust follows the Prevent element of the Government's Counter Terrorism Strategy, and where deemed appropriate, will seek external support for any member(s) of the Trust community* through referral to the Channel Programme. This programme aims to work with the individual to address their specific vulnerabilities, prevent them becoming further radicalised and possibly entering the criminal justice system because of their actions. It is recognised that radicalisation can occur to an individual from any section of society and is not particular to any racial, ethnic or social group. It is further recognised that in many instances the process of radicalisation is essentially one of grooming by others.

*Any individual(s), pupil(s) or adult(s), that Trust employees come into contact with in the course of their work.

7. The Academies Curriculum and Tools for Learning

7.1 Internet use

Pupils will be taught how to use online digital technologies safely and responsibly, for researching information, exploring concepts, deepening knowledge and communicating effectively in order to further learning. This will be through both Computing and PSHE lessons and across the curriculum.

The following concepts, skills and understanding will be taught:

- internet literacy, including making good judgements about websites
- understanding risks such as viruses and opening mail from a stranger
- knowledge of copyright, plagiarism, file-sharing and downloading illegal content issues
- data privacy awareness – knowing what is and is not safe to upload
- how to access to appropriate guidance, where to go for advice and how to report abuse

These skills and competencies will be taught within the curriculum so that pupils have the security to explore how online technologies can be used effectively and in a safe and responsible manner. Pupils will know how to deal with any incidents with confidence.

7.2 Academy Staff Email and Mobile Phone Usage

Academy/Trust staff can communicate with the parents of pupils via their academy/trust email address or provided work phone following clear protocols and rules. All such communications must be:

- Professional and related to school matters only
- Reflect a suitable tone/content and ensure that the good name of the school is maintained

- Only sent between 8am and 6pm on days when a school is open to pupils

There are systems in place for storing all electronic communications which take place between school and parents/pupils. These can be monitored and checked as required.

If these rules are broken by a member of staff parents should report this to a Vice-Principal or the Principal. If they are broken by a parent, the parent may be required to make all future communications through the main school admin/contact email address.

Primary age pupils must never be contacted directly by any means other than by Academy set-up/approved systems such as Seesaw.

Secondary age pupils may be appropriately (as above) communicated with via their school provided email addresses.

Under no circumstances will staff contact students, parents or conduct any school business using a personal email address or non-work provided phone. Responsible use of staff personal email accounts on school systems is permitted outside teaching hours.

Staff should not use personal phones in classrooms or other areas of the school setting where they are with pupils. Staff should not use their personal phones to contact parents or other staff within work unless directed to do so by Principal / Senior Manager in exceptional circumstance where a work provided phone is not available. The aforementioned exceptional circumstance requires the staff member to hide their number. Staff must never contact pupils using their personal phones.

Staff must not use personal devices to take any photos or videos at work. Academy / Trust provided devices are made available for this purpose. Any photos or videos taken must comply with Section 8.

Certain applications such as Microsoft Authenticator on personal phones are required to be used by all staff for access to Academy / Trust systems.

7.3 Academy Pupils' Mobile Phones & other Electronic Devices or Accessories

Primary phase pupils: without the express permission of a Principal/Vice-Principal pupils use of mobile phones is not allowed in the Academies or on school grounds during the school day, at after-school clubs, on a school trip or residential visit. Pupils may leave mobile phones in the main school office for the day. Sanctions, such as removing a pupil's right to have a device on the school premises, will be taken in the event of inappropriate use.

Secondary phase pupils: mobile phone/any other electronic devices or accessories must not used, seen or heard during the school day. Sanctions, such as removing a pupil's right to have a device on the school premises, will be taken in the event of inappropriate use.

Unauthorized or secret use of a mobile phone or other electronic device, to record voice, pictures or video is forbidden. Publishing of such material on a web site which causes distress to someone will be considered a breach of school discipline, whether intentional or unintentional. The person responsible will be expected to remove this immediately upon request. If the victim is another student or staff member it is not a defence that the activity took place outside school hours.

The sending or forwarding of text messages, emails or other online communication deliberately targeting a person with the intention of causing them distress or harm is online bullying; this will be considered a disciplinary matter.

The Education Act 2011 gives school's the power to confiscate/search the contents of any mobile device if the Principal believes it contains any material that could be used to bully or harass others. It should be made clear to staff, students and parents that the Principal has the right to examine content on a mobile phone or other personal device to establish if wrongdoing has occurred.

Wearable technology must not to be worn during the school day, tests or examinations.

8. Photographs and video
The term 'image' refers to the taking of photographs or video via any camera or other technology.

Academy images of pupils will not be in any way compromising or inappropriate. If a member of staff is unsure if a photograph is appropriate for publication, they should seek guidance from the e-Safety Leader, a Vice-Principal or the Principal.

Images of pupils may only be uploaded online by staff if parents/carers have given their permission for this. Online image filenames must not identify pupils.

Images/video of pupils can only be taken on Academy devices and then must be stored securely on the school network, never on personal devices such as mobile phones.

8.1 Photographs and video – Parents/Carers
Parental Photography and Video Recording at Academy Events
Parents and carers are welcome to take photographs or video recordings at school performances and events, provided the following conditions are met:

- Only images of your own child/children may be captured.
- These images or videos must be used strictly for personal, family, or close friend sharing.
- Images or video recordings must not be posted on social media platforms or shared online, in line with data protection and safeguarding guidance.
- Staff will inform parents/carers in advance and at the start of events whether photography or video recording is permitted. This decision may be influenced by factors such as performance licensing or copyright restrictions.

In all cases:

- No commercial use, public distribution, or publication of any recordings or images is permitted.
- Consent from other parents/carers, pupils, or staff must not be assumed.

Outside of performances and events:

- Parents/carers must seek permission from a member of staff before taking photographs or videos on academy premises.
- The same conditions as listed above apply.

This guidance is in line with UK GDPR, The Data Protection Act 2018, and safeguarding protocols across the Trust.

9. Safeguarding and Security Measures
Our Academies broadband connectivity has strict filtering systems to resist the delivery of inappropriate content (including extremist and terrorist materials). Anti-virus and

malware/spyware software is on our networks and updated on a regular basis. A firewall is used to protect our networks, including all information about pupils, from access by unauthorised users. Our wireless networks have encryption codes to resist hacking. Regular backups are made of all key Trust data.

10. Remote education and Home Learning

In response to emergency closures or a pupil needing to be educated off-site schools may use
online learning resources such as Seesaw, Zoom, MS Teams, Google Classroom, Sparx.

These will be used as necessary in circumstances where a child or group of children must quarantine or self-isolate, or when the school needs to close in an emergency for any reason.

All Acceptable Use Policies will apply to school resources which are accessed in the home environment. An additional Acceptable Use Policy will be used if remote education takes place which involves live online contact between teachers and students using a webcam or text messaging app/software.

Parents and carers will be informed of the online resources pupils are expected to access and which staff students will communicate with their children online.

The following DfE guidance will be used:
https://www.gov.uk/guidance/safeguarding-and-remote-education
(DfE November 22)

Appendix 1. Trust-wide Digital Security

Effective digital security depends not only on technical measures, but also on the following of appropriate policies and procedures and on good user education and training. All employees/governors who have access to the Trust's IT systems must undertake NCSC Cyber Security Training. Employees/governors will be told how this training should be accessed and their understanding/accreditation and agreement with its requirements recorded.

The Trust is responsible for ensuring that its infrastructure is as safe and secure as is reasonably possible:

- users can only access data to which they have a work need, adhering to the principle of least privilege*
- access to personal data is securely controlled in line with the Trust's data policies
- logs are maintained of access by users and of their actions while users of the system
- systems will be managed to ensure that the Trust meets recommended technical requirements**
- there are regular reviews of the safety and security of Trust computer systems

* All Trust employee accounts must be created with standard access, if any member of staff requires any privilege elevation this must be agreed by either an Academy Principal, the Trust CFOO or Senior IT Team, details must be recorded for future reference.

** Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the Trust's systems and data. Responsibilities for the management of technical security are clearly assigned to appropriate and well-trained IT staff who may employ suitably qualified and accredited third-party IT support companies.

Trust-wide Policy and Procedures:

Each Trust employee is responsible for the security of any Trust usernames and passwords they use. They must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

- Good practice highlights that passwords over 16 characters in length generated by using a combination of unconnected words are extremely difficult to crack. Password length trumps any other special requirements such as uppercase/lowercase letters, number and special characters. Passwords should be easy to remember, but difficult to guess or crack (do not include names or any other personal information that might be known by others).
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of the Trust.
- Passwords must be changed on first login to the system and then at least on an annual basis. Users must change their password immediately if it is in any way potentially or actually compromised.
- The use of a secure password vault solution is acceptable and recommendations can be obtained from technical teams.
- Suitable arrangements should be in place to provide temporary staff/visitors with appropriate access to systems which then expires after use.

Devices supplied to Trust employees should only be used by the employee (e.g. not used as a shared family device).

Removable media (e.g., memory sticks and portable drives) must be supplied by Academies/the Trust with the authorisation of the IT Team. All removable devices require encryption.

The installation of apps/programs should be requested via the ICT Helpdesk system and will be accommodated when possible, in line with security best practices.

Filtering:

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate. Filtering systems cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use.

All users have a responsibility to report immediately to their senior management team any believed failings in Trust filtering which they become aware e.g. any sites/content that is accessed which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials. A monitoring process alerts each Academy/The Trust to breaches (attempted or actual) of the filtering policies, such breaches will then be investigated and acted upon.

Personal mobile devices are not permitted access to Trust networks without authorisation from the IT Team / Principal / CFOO.

In the event of any legitimate need to switch off any degree of the filtering for any user by technical support staff this must be logged and carried out by a process that is agreed by a Principal, the Trust IT Infrastructure Manager or the Trust CFOO.

Procedures Following Cyber Attack or Data Breach

Types of data breach include:

- **Malware:** a virus on a device
- **Ransomware:** a hacker gains control and encrypts the system then leaves a ransom note
- **Password attack:** a hacker tries multiple passwords to gain access
- **Phishing**: an email or phone call that seems legitimate to get financial or personal information
- **Lost/stolen device/memory stick:** this could contain sensitive information.
- **Misplaced pupil information:** e.g., on a school visit with pupil details/medical information
- **Sending personal data to the incorrect email recipient**

Staff must never try and cover such an incident up and hope no one finds out.
Staff must always report any incident no matter how insignificant they think it is.
This applies to all employees on the Trust.

If you suspect a data breach of any sort you must inform the CFOO immediately. If the CFOO is not available then inform the Trust IT Infrastructure Manager or another member of the Trust Central Team. If it does constitute a data breach the Trust has 72 hours in which to inform the Information Commissioner Officer (ICO).

Once reported please ensure you log as much information as possible:

- The date, time, details of incident* and those involved
  *The nature of the breach. Was it:
  Digital – e.g. hacking, virus, ransomware, file corruption.
- **Electronic** - e.g., lost laptop, phone, USB.
- **Verbal** - e.g., wrong information given over the phone.
- **Paper** - e.g., lost or misplaced file(s)

You take photographs of any messages you receive that are suspicious and share with the CFOO

- Do not delete anything – preserve the evidence
- Do not switch anything off – you may need to disconnect the internet or disable remote access but seek advice
- Assess the breach: can you determine what information may have been lost/taken? Make a list of all possibilities.
- If applicable, check around site to see if anyone else has been affected

The CFOO/Central Team will direct your next steps and will report to the respective agencies.

Appendix 2a. Digital Technologies - Agreed Usage Rules for Staff

To ensure that all adults within the Trust are aware of their responsibilities when using any digital/online technologies they are asked to sign their agreement to specific Agreed Usage Rules.
This is both to protect the Trust and is a safeguard for individuals from any potential allegations or inadvertent misuse.
These rules apply to all digital/online technology usage and to anything that may be downloaded or printed.

General:

- I have read, understood, agree and will comply with the procedures within the Trust-wide 'Use of Digital Technologies Policy' and the Trust's approach to Digital Security (Appendix 1).
- I will only use Trust/Academy devices/systems in an appropriate manner and for work-related uses, any personal use requiring the approval of a senior manager.
- I will ensure that I keep all passwords secure and try not to leave any device/account 'logged in'.
- I will take measures or seek advice to prevent the potential introduction of viruses to the network.
- I will exercise caution when following links/opening attachments within emails, alert to signs of cyber-attack.
- I will adhere to copyright and intellectual property rights.
- I will report any accidental misuse and report any incidents of concern to a senior manager.

Photographs, Video & Mobile file storage:

- Teaching staff - I understand that I need to oversee and manage pupils' uploading of content (including photographs or video) to the internet (including school provided online environments such as Seesaw). I know that all Academy images should appropriate and beyond first names not reveal any personal information about pupils if uploaded to the internet.
- All staff - I must only use equipment provided by the Trust/Academy. Media taken on Trust/Academy portable devices should be transferred to the school network/school provided online environment as soon as is possible. Any use of personal equipment, including mobile phones, for taking photographs/video is strictly prohibited.
- All staff - I must only use Trust/Academy provided storage devices and follow agreed encryption procedures. I will not download, copy or store any Trust data (including pupil photographs) to a personal device.

Communication & Social Networking:

- I will only use my Trust/Academy email address for work-related communications.
- I will ensure all messages are written carefully and politely (emails can be forwarded to unintended readers) and will secure any emails or password protect any email attachments which contain personal information.
- Academy staff - I will never use a personal phone to contact pupils and only if directed to/with my number hidden, to contact parents. Emails to parents must be sent from a staff member's Trust email address, be professional and related to school matters only plus only sent between 8am and 6pm on days when a school is open to pupils. Secondary phase pupils school email addresses may be emailed under the same terms.
- Academy staff - I realise that I am putting myself at risk of misinterpretation and allegation should I contact pupils via any systems other than Academy provided ones. I will not use any non-Academy online technologies to communicate with pupils.
- I understand the value of setting my 'Privacy' settings appropriately on any social networking site and not stating my place of work – this will help to prevent unacceptable 'friendship' requests.
- I will not accept or request the 'friendship' of pupils (or ex-pupils).
- I will not risk bringing the Trust/my Academy into disrepute by 'discussing any aspect of my work or by making any Trust/Academy related comments or references' online (or by any means to non-Academy personnel, to ensure others do not do the same) other than (as delegated) via official Trust/Academy web presence agreed protocols.

I have read, understood and will follow the Trust's 'Use of Digital Technologies Policy' and the rules specified above.
I understand my responsibilities regarding safeguarding children when digital/online technologies are used.

Signed: _____ Date: _____

Name (printed): _____

Appendix 2b. Digital Technologies – Agreed Usage Rules for Staff
Abridged - for short-term staff / volunteers / work experience students

To ensure that all adults within the Trust are aware of their responsibilities when using any digital/online technologies they are asked to sign their agreement to specific Agreed Usage Rules.
This is both to protect the Trust and is a safeguard for individuals from any potential allegations or inadvertent misuse.
These rules apply to all digital/online technology usage and to anything that may be downloaded or printed.

General:

- I will only use Trust/Academy devices/systems in an appropriate manner and for work-related uses, any personal use requiring the approval of a senior manager.
- I will take measures or seek advice to prevent the potential introduction of viruses to the network.
- I will ensure that I keep all passwords secure and try not to leave any machine 'logged in'.
- I will report any accidental misuse.
- I will adhere to copyright and intellectual property rights.
- I will report any incidents of concern to a Senior Manager.

Photographs & Video:

- All staff - I must only use equipment provided by the Trust/Academy. Media taken on Trust/Academy portable devices should be transferred to the school network/school provided online environment as soon as is possible. Any use of personal equipment, including mobile phones, for taking photographs/video is strictly prohibited.
- All staff - I must only use Trust/Academy provided storage devices and follow agreed encryption procedures. I will not download, copy or store any Trust data (including pupil photographs) to a personal device.

Communication & Social Networking:

- Academy staff - I realise that I am putting myself at risk of misinterpretation and allegation should I contact pupils via any systems other than Academy provided ones which I have been authorised to use. I will not use any non-Academy online technologies to communicate with pupils. I will not use a personal phone to contact pupils or parents.
- I understand the value of setting my 'Privacy' settings appropriately on any social networking site and not stating my place of work – this will help to prevent unacceptable 'friendship' requests.
- I will not accept or request the 'friendship' of pupils (or ex-pupils).
- I will not risk bringing the Trust/my Academy into disrepute by 'discussing any aspect of my work or by making any Trust/Academy related comments or references' online (or by any means to non-Academy personnel, to ensure others do not do the same).

I have read, understood and agree to follow the Trust's rules as specified above.
I understand my responsibilities regarding safeguarding children
when digital/online technologies are used.

Signed: _____ Date: _____

Name (printed): _____

Appendix 3a. Digital Technologies - EYFS/KS1 Usage Guidance/Rules

Computing Rules for School and Advice for Home

Smartphones, tablets and the internet can be great!

They can be helpful and fun for everyone in many different ways.

Being upset when you're using them doesn't happen often but isn't nice. By following a few simple rules we should all be happy and safe at school and at home.

In Reception we met Smartie the Penguin who taught us what to do if we were unsure or worried.

We know which grown-ups we can trust

and can always ask them for help.

As we get older we will learn more,
with the help of grown-ups we trust,
about always using digital devices and the internet safely:

- I will take care of digital devices, holding and using them carefully
- I'll let other people use digital devices when it's their turn
- I will only use apps and websites that I'm supposed to
- I will stop using equipment and listen if someone wants to talk to me
- If I'm unsure what to do I will ask a trusted grown-up for help
- If something worries me I will tell a trusted grown-up straightaway
- I will only ever send polite, friendly and helpful messages
- I will not reply to unpleasant messages
- I will never arrange to meet people I don't know
- I will not share information about myself or other people on the internet
- I will always ask a trusted grown-up before uploading any photographs

Appendix 3b. Digital Technologies - KS2 Usage Guidance/Rules

Computing Rules for School and Advice for Home

Digital devices and the internet are a great resource
and they can be helpful to everyone in many different ways.
They have become a near-essential tools for learning, for communication and for use in later life.

Bad experiences and events are relatively rare but can be serious and upsetting.
By following a few simple rules these can be avoided.
It is important that we all understand these rules to be happy and safe at school and at home.

As a pupil, with the help of adults I can trust (my parents/carers and my teachers)
I agree to the following rules to use digital devices and the internet safely:

- I will take care of digital devices, holding and using them carefully
- I'll let other people use digital devices when it's their turn
- I will only use apps and websites that I'm supposed to
- I will stop using equipment and listen if someone wants to talk to me
- Everything I do on the internet must be approved by a trusted adult
- If I'm unsure what to do I will ask a trusted adult for advice
- If something worries me I will tell a trusted adult straightaway
- Apart from my trusted adults I will keep my passwords secret
- I will check that information I find on the internet is reliable
- I will not copy things off the internet and pretend I made them
- I will only ever send polite, friendly and helpful messages
- I will not reply to unpleasant messages
- I will never arrange to meet people I don't know
- I will not share information about myself or other people on the internet
- On public-facing sites my usernames should not give information about me
- I will always ask a trusted adult before uploading any photographs
- I will not open attachments or download files unless I trust who they're from

Appendix 4. Digital Technologies - KS3/KS4 Pupil Agreed Usage Rules

Digital Technologies - KS3/KS4 Pupil Agreed Usage Rules

I understand that use of the internet and electronic communication is granted to me as a privilege in return for my acceptance of this agreement.

Any misuse on my part may result in loss of that privilege and other sanctions being taken. This also applies to any activity undertaken outside the Academy which contravenes the acceptable use rules of the Academy.

All my online activity will be appropriate to:

- Ensure the safety and security of the Academy network and systems
- Ensure respect for all members of the community
- Maintain the reputation of the Academy

In particular this means:

- I will only access the Academy's IT system and internet via my authorised account and password, which I will not make available to others
- I will ensure that I do not willfully damage the Academy's network by means of malicious code (e.g. virus infections, malware), hacking or physical tampering
- Language which I use in electronic communication will be appropriate/suitable, as for all school work
- I will respect copyright of all materials
- I will not willfully interfere with and/or delete another person's work files
- I will not send or forward messages, publish or create material which is offensive, hurtful or otherwise upsetting to another person. Nor will I post anonymous messages or forward chain letters
- I will not use a mobile phone, camera or other electronic device to take, publish or circulate pictures or videos of anyone without their permission

In addition I understand that:

- Use of the network to knowingly access inappropriate materials such as pornographic, racist, homophobic or offensive material is forbidden and may constitute a criminal offence
- Work submitted electronically will be checked against online publication repositories and banks of student work for plagiarism. Work will also be checked for generation by AI tools e.g. ChatGPT.
- Guidelines for safe use of the internet must be followed and I will report any materials or conduct which I feel is unacceptable

In particular the following is deemed unacceptable use or behaviour by students (this list is non-exhaustive):

- Visiting internet sites that contain obscene, hateful or other illegal material;
- Using the computer to perpetrate any form of fraud, or software, film or music piracy;
- Using the internet to send offensive or harassing material to other users;
- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence;
- Hacking into unauthorised areas;
- Creating or transmitting defamatory material;
- Deliberately or recklessly introducing any form of computer virus into the academy's network.
- The Academy will monitor all internet and email activity to examine or delete any files that may be held on its computer system, to monitor and, if necessary to report anything which may constitute a criminal offence. The Academy has the right to confiscate and or search for electronic devices and if necessary to hand over to the police.

Student's full name: _____ Year Group: _____

Signed: _____ Date: _____

Appendix 5a. Procedures Following Staff Incident or Misuse

Principals / the Trust COO will ensure these procedures are followed:

A. **An inappropriate website is accessed accidentally:**
Report incident/website to a Vice-Principal, a Principal or the Trust COO.
Incident logged and technical team informed to update filtering service.

B. **An inappropriate website is accessed deliberately:**
Ensure that no one else can access the material (switch off the display/remove the tablet)
If possible, preserve any evidence.
Report immediately to a Vice-Principal, a Principal or the Trust COO.
Contact Police or other agencies (including the Channel Scheme re. radicalisation) as necessary.
Decide on appropriate disciplinary response.
Incident logged and technical team informed to update filtering service.

C. **A staff member has received an inappropriate communication:**
Do not forward this communication/material to anyone else – doing so could be an illegal activity.
Immediately alert a Vice-Principal, a Principal or the Trust COO.
Vice-Principal, Principal or Trust COO to preserve any evidence and log the incident.
Contact Police or other agencies, as for B.

D. **A staff member has used ICT equipment inappropriately:**
Ensure that no one else can be affected by the activity (switch off the display/remove the tablet).
If possible, preserve any evidence.
Report to a Vice-Principal, a Principal or the Trust COO immediately.
If involving pupils also the Designated Person for Child Protection to follow Child Protection Policy and inform parents/carers.
Contact Police or other agencies, as for B.
Decide on appropriate disciplinary response.

E. **A staff member has communicated with a pupil inappropriately:**
Ensure the pupil is reassured and remove them from the situation immediately.
Report to the Principal / Designated Person for Child Protection.
Preserve the information received by the pupil if possible.
Principal to follow the Allegation Procedure and/or Child Protection Policy.
Notify parents/carers.
Contact CEOP / Police or other agencies, as for B.
Decide on appropriate disciplinary response.

F. **Inappropriate, damaging, malicious or threatening comments/files are posted online:**
Preserve any evidence. Support any individuals affected.
Inform a Vice-Principal, a principal or the Trust COO immediately.
Investigate. Decide on appropriate remedial actions.
Contact Police or other agencies as for B.
If posted by staff member decide on appropriate disciplinary response.

G. **Any misuse or breach of the acceptable use policy which may risk the security of any personal data should be reported to the Trust Data Protection Officer via the COO.**

N.B. There are **events which must be reported directly to the police**:

- Indecent images of children found.
- The sending of obscene materials to a child.
- Suspicion of 'grooming' behaviour.

CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if such an event occurs. If in doubt, do not power down the machine.

Appendix 5b. Procedures Following Pupil Incident or Misuse

Principals will ensure these procedures are followed:

A. **An inappropriate website is accessed accidentally:**
Ensure that no one else can access the material (switch off the display/remove the tablet).
Reassure the pupil that they are not to blame and praise/support them (or 'informant' peer) for being safe and responsible by telling a member of staff.
Report the incident/website to a Vice-Principal or the Principal.
Decide if parents/carers need to be notified.
Incident logged and technical team informed to update filtering service.

B. **An inappropriate website is accessed deliberately:**
Ensure that no one else can access the material (switch off the display/remove the tablet).
Report incident /website to a Vice-Principal or the Principal.
Notify parents/carers.
Notify external agencies (including the Channel Scheme re. radicalisation) as necessary.
Decide on appropriate sanction(s).
Incident logged and technical team informed to update filtering service.

C. **A Pupil has received an inappropriate communication:**
Ensure the pupil is reassured and remove them from the situation immediately.
Preserve the communication/all related evidence as received by the pupil.
Report to the Principal / Designated Person for Child Protection.
Follow the Child Protection Policy.
Notify parents/carers plus contact CEOP / Police and other agencies, as for B.

D. **A Pupil has used ICT equipment inappropriately:**
Ensure that no one else can be affected (switch off the display/remove the tablet).
Report to a Vice-Principal or the Principal immediately.
If involving other pupils the Designated Person for Child Protection to follow Child Protection Policy and inform parents/carers.
Notify parents/carers plus contact other agencies, as for B, if necessary.
Decide on appropriate sanction(s).

E. **Inappropriate, upsetting, malicious or threatening comments/files are posted online:**
Preserve all related evidence. Support any individuals affected.
Report to the Principal / Designated Person for Child Protection.
Decide on appropriate remedial actions.
If posted by a pupil decide on appropriate sanctions.
Notify parents/carers and other agencies, as for B.

F. **Any misuse or breach of the acceptable use policy which may risk the security of any personal data should be reported to the Trust Data Protection Officer via the COO.**

Appendix 6. National Guidance

The following national guidance is acknowledged and included as part of our Use of Digital Technologies Policy:

Keeping Children Safe in Education

(DfE 2024)

Teaching Online Safety in School
(DfE 2023)

The Prevent Duty: for schools and childcare providers
(DfE 2023)

Revised Prevent Duty Guidance for England and Wales
(Home Office 2024)

Cyberbullying: Advice for Principals and School Staff
(DfE 2017)

Sharing nudes and semi-nudes: advice for education settings working with young people
(DfE 2024)

Data Protection Act 2018

The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020

Computer Misuse Act 1990

Human Rights Act 1998

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

Education Act 2011

Freedom of Information Act 2000

Education and Inspections Act 2006

Searching, screening and confiscation: advice for schools 2022

National Cyber Security Centre (NCSC): Cyber Security for Schools

Education and Training (Welfare of Children) Act 2021

UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Meeting digital and technology standards in schools and colleges