Use of Digital Technologies Policy

2024

This is a Trust-wide Policy which applies to
all academies, designations, staff and pupils within the Trust

Version Control:

Version 1 - Adapted from Northamptonshire County Council's AUP "which schools and other children's services can download and adapt to suit their needs," by TB, 19/10/09.

Version 2* - Significantly updated to reflect changing technologies, needs, school systems and procedures, by AB and JP, February/March 2012*

Version 3* - Updates/clarifications by JP: May 2015*, January 2017*, May 2017*, October 2017*, May 2018*,
March 2019*

Version 4* - Trust-wide updates/clarifications by JP: September 2021

Version 5* - Addition of Trust-wide IT Security appendix by JP: April 2022

Version 6* - Updated by JP to cover full 2-18 delivery offer: May 2023

Version 7* - Updated by JF, AH & AM to include new legislation October 2024

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.

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.

Introduction and aims

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

However, the ICT resources and facilities our Trust uses could also pose risks to data protection, online safety and safeguarding.

This policy aims to:

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

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

Breaches of this policy may be dealt with under our disciplinary policy.

Relevant legislation and guidance

Keeping Children Safe in Education (DfE 2024)

Teaching Online Safety in School (DfE 2019)

The Prevent Duty: for schools and childcare providers (DfE 2015)

Revised Prevent Duty Guidance for England and Wales (Home Office 2015)

Cyberbullying: Advice for Principals and School Staff (DfE 2014)

Sharing nudes and semi-nudes: advice for education settings working with young people (DfE 2020)

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

Definitions

- **ICT facilities**: 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 that may become available in the future which is provided as part of the Trust's ICT service
- **Users**: anyone authorised by the Trust to use the ICT facilities, including trustees, governors, staff, pupils, volunteers, contractors and visitors
- **Personal use**: any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user

- **Authorised personnel**: employees authorised by the Trust to perform systems administration and/or monitoring of the ICT facilities
- **Materials**: files and data created using the Trust's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 6 for a glossary of cyber security terminology.

Roles and Responsibilities within a Trust Academy:

Roles: Trust Boards, Principals, Heads of School and Vice-Principals

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

- The Principal / Head of School 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 / Head of School 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 / Head of School 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.

Roles: Trust IT Digital Infrastructure Manager and Academy e-Safety/Digital Security Leaders

It is the role of the Trust ITnDigital Infrastructure Manager with designated e-Safety/Digital Security Leaders to:

- Liaise with the PSHE, Safeguarding 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 / Head of School on a regular basis.

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/Safeguarding 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 / Head of School. In the event of an allegation made against the Principal or Head of School 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.
- Monitor pupil's choices of usernames within any online environments.
- 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.

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.
- Use caution and measures such as installed anti-virus software to prevent the transfer of viruses to a Trust network from removable media and the internet.
- 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.
- Only use Academy/Trust provided USB memory sticks 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.

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.

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 IT Digital Technology usage requirements – see Appendix 4.

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.

Unacceptable use

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

Unacceptable use of the academy's ICT facilities includes:

- Using the academy's ICT facilities to breach intellectual property rights or copyright
- Using the academy's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the academy's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the academy into disrepute
- Sharing confidential information about the academy, its pupils, or other members of the academy community
- Connecting any device to the academy's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the academy's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the academy's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the academy's ICT facilities
- Causing intentional damage to the academy's ICT facilities
- Removing, deleting or disposing of the academy's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the academy
- Using websites or mechanisms to bypass the academy's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- Using AI tools and generative chatbots (such as ChatGPT and Google Bard):
- During assessments, including internal and external assessments, and coursework
- To write their homework or class assignments, where AI-generated text or imagery is presented as their own work

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

Exceptions from unacceptable use

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

Pupils may use AI tools and generative chatbots:

- As a research tool to help them find out about new topics and ideas
- When specifically studying and discussing AI in schoolwork, for example in IT lessons or art homework about AI-generated images. All AI-generated content must be properly attributed

Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies on behaviour and staff code of conduct. The Great Heights Trust reserves the right to revoke access to any system.

Staff (including trustees, governors, volunteers, and contractors)

Access to academy ICT facilities and materials

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

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

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

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the IT Digital Infrastructure Manager or IT Team.

Requests to access files / facilities are logged via the ticketing system, approvals where necessary are sent to line managers / SLT.

Use of phones and email

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

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

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

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

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

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

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

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

If staff send an email in error that contains the personal information of another person, they must inform the IT team and school business or administration manager immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or pupils. Staff must use phones provided by the school to conduct all work-related business. If a personal phone must be used staff should ensure their number is withheld.

School phones must not be used for personal matters.

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

The school can record incoming and outgoing phone conversations.

If you record calls, callers must be made aware that the conversation is being recorded and the reasons for doing so. Your academy's phone system probably has an automated option you can use/adapt.

Explain when you record phone conversations and why. For instance:

- "All calls to the school office are recorded to aid administrators"
- "Calls are recorded for use in staff training"

Staff who would like to record a phone conversation should speak to the school office.

All non-standard recordings of phone conversations must be pre-approved, and consent obtained from all parties involved.

Protocol for approving:

- Discussing a complaint raised by a parent/carer or member of the public
- Calling parents/carers to discuss behaviour or sanctions
- Taking advice from relevant professionals regarding safeguarding, special educational needs (SEN) assessments, etc.
- Discussing requests for term-time holidays

Personal use

Staff are permitted to occasionally use academy ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The Trust IT Team or Senior Leadership may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

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

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

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

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's [mobile phone/personal device policy].

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

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

Personal social media accounts

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

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

Remote access

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

Staff can remotely access sites via either a remote desktop platform or academy provided VPN.

- The IT team manages who access' resources offsite.
- The security of these systems complies with our data protection policy. 2 Factor Authentication is in place for all remote access systems.
- Staff can request remote access via the Trust ticketing system.

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

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

Academy social media accounts

The school has an official Facebook, Twitter and other social media accounts, managed by the trust marketing team. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

The Trust has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

Monitoring and filtering of the Trust's network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the Trust reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

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

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. The trust uses Smoothwall firewall and filter to monitor and inspect all traffic within its academies.

The Trust monitors ICT use in order to:

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

LGB's are responsible for making sure that:

- The academy meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
    - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The academy's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the academy's DSL and ICT manager, as appropriate.

Pupils

Access to ICT facilities

Computers and equipment in the school's ICT suite/ICT stores are available to pupils only under the supervision of staff.

Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff.

Pupils will be provided with an account linked to the school's virtual learning environment, which they can access from any device by using the following URL "teams.microsoft.com".

Sixth-form pupils can use the computers in silent study independently, for educational purposes only.

Search and deletion

Under the Education Act 2011, the Principal / Head of School, and any member of staff authorised to do so by the Principal/ Head of School, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the academy rules as a banned item for which a search can be carried out (your behaviour policy should list these items), and/or
- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the principal / head of school / designated safeguarding lead / appropriate member of staff.
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation (if the pupil refuses to co-operate, you should proceed according to your behaviour policy)

The authorised staff member should:

- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item.

- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:

- Cause harm, **and/or**
- Undermine the safe environment of the academy or disrupt teaching, **and/or**
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / Principal / Head of School/ other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider whether the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as is reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, **and/or**
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- **Not** copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy.

Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the academy complaints procedure.

Unacceptable use of ICT and the internet outside of school

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

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

See above and our academy's behaviour/discipline policy.

Parents/carers

Access to ICT facilities and materials

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

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

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

Communicating with or about the academy online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents/carers play a vital role in helping model this behaviour for their children, especially when communicating with the academy through our website and social media channels.

We ask parents/carers to sign the agreement in appendix 2.

Communicating with parents/carers about pupil activity

The academy will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out.

When we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents/carers in the same way that information about homework tasks is shared.

In particular, staff will let parents/carers know which (if any) person or people from the academy pupils will be interacting with online, including the purpose of the interaction.

Parents/carers may seek any support and advice from the academy to ensure a safe online environment is established for their child.

Data security

The academy is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.

Staff, pupils, parents/carers and others who use the academy's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

Passwords

All users of the academy's ICT facilities should set strong passwords for their accounts and keep these passwords secure. Passwords should be complex, not include personally identifiable information or similar information.

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

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

Software updates, firewalls and anti-virus software

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

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

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

Data protection

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

Access to facilities and materials

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

These access rights are managed by the IT Infrastructure Manager

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

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

Encryption

The academy makes sure that its devices and systems have an appropriate level of encryption.

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

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

Protection from cyber attacks

Please see the glossary (appendix 8) to help you understand cyber security terminology.

The academy will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details
    - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:

  - **Proportionate**: the academy will verify this using a third-party audit at least annually, to objectively test that what it has in place is effective
  - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
  - **Up to date**: with a system in place to monitor when the academy needs to update its software
  - **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be
- Back up critical data daily and store these backups on cloud-based backup systems / external hard drives / NAS Drives that aren't connected to the school network and which can be stored off the school premises.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our IT department.
- Make sure staff:
  - Dial into our network using a virtual private network (VPN) when working from home
  - Enable multi-factor authentication where they can, on things like academy email accounts
  - Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the academy has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT department including, for example, how the academy will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested yearly and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
- Work with the Trust to see what it can offer the academy regarding cyber security, such as advice on which service providers to use or assistance with procurement.

Internet access

The academy's wireless internet connection is secure.

- Filtering is used on all wireless systems.
- Separate networks are in use to separate devices and use cases.

Inappropriate sites and content that are identified

While the Trust employs comprehensive web filtering, it is acknowledged that no system is infallible. Staff are required to report any instances of inappropriate content that bypass the filter, or any legitimate websites that are incorrectly blocked, via the Trust's ticketing system. In the event of a serious incident, this must be escalated immediately to the Trust IT Lead

Parents/carers and visitors

Parents/carers and visitors to the school will not be permitted to use the academy's WiFi unless specific authorisation is granted by the Principal.

The Principal will only grant authorisation if:

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

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

Monitoring and review

The Principal / Head of School and IT team monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the academy.

This policy will be reviewed every year.

Related policies

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

- Online safety
- Social media
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection
- Mobile phone usage

Appendix 1: Facebook cheat sheet for staff

Do not accept friend requests from pupils on social media

10 rules for staff on Facebook

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

Check your privacy settings

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

What to do if …

A pupil adds you on social media

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

A parent/carer adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
  - Responding to 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other staff at the school
  - Pupils may then have indirect access through their parent/carer's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent/carer know that you're doing so

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

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

Appendix 2. 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*
- 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 or the Trust COO, 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 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. 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.

Where personal mobile devices are allowed internet access through the Trust networks, filtering will be applied that is consistent with the above Trust approaches.

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 Digital Infrastructure Manager or the Trust COO.

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 of the Trust.

If you suspect a data breach of any sort you must inform the COO immediately. If the COO is not available then inform the Trust IT Digital 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 COO
- 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 COO/Central Team will direct your next steps and will report to the respective agencies.

Appendix 3a. 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 blocked, 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 3b. 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 4a. 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 4b. 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 5. 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: _____

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 6b. 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 7. 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 2019)
The Prevent Duty: for schools and childcare providers
(DfE 2015)
Revised Prevent Duty Guidance for England and Wales
(Home Office 2015)
Cyberbullying: Advice for Principals and School Staff
(DfE 2014)
Sharing nudes and semi-nudes: advice for education settings working with young people
(DfE 2020)

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

Appendix 8. Glossary of cyber security terminology

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

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.

TERM	DEFINITION
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.