ICT and internet acceptable use policy (Including cyber-attacks)

Reviewed By	**R Leonard**
Approved by/when	**September 2024 Executive Leadership Team**
To be reviewed	**September 2026**

Document Control	
Title	Acceptable use of ICT Policy (Including Cyber Security)
Date	September 2024
Supersedes	Acceptable use of ICT Policy (Including Cyber Security) September 2022
Amendments	Section 2. Relevant legislation and guidance – added KCSIE 2024 and nudes and semi nudes guidance Section 4. Added section on unaccaptable use of AI by pupils Section 5. Split use of e mail and mobile phone to make the section clearer and to align with mobile phone policy and trust declaration Section 5.5 Added the role of governors regarding filtering and monitoring Section 6.2 Added to and updated the section on role of staff when conducting searches of mobile devices or confiscation of devices Section 6.3 Added nudes or semi nudes to list of unaccpetable use Section 7.3 Updated the section on how and what we communicate with parents Section 8 Updated the secion on data security Section 9 Updated that the central leadership team will monitor the security of any internal system. Changed from Director of Buisness Operations

Contents

1. Introduction and aims

At the Bolton Impact Trust we:

Believe everyone can achieve

Inspire a love of learning

Transform potential into long lasting success

ICT is an integral part of the way our academies work, and is a critical resource for pupils, staff, governors, trustee's volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of each academy.

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

This policy aims to:

- Set guidelines and rules on the use of The Trust's ICT resources for staff, pupils, parents, governors and trustees
- Establish clear expectations for the way all members of the trust community engage with each other online
- Support the trust and academy policies on data protection, online safety and safeguarding
- Prevent disruption to the trust and its academies 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 governors, trustees, staff, pupils, volunteers, contractors and visitors.

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

2. Relevant legislation and guidance

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

- 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
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2024
- 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

3. Definitions

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

4. Unacceptable use

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

Unacceptable use of the trust's ICT facilities includes:

- Using the trust's ICT facilities to breach intellectual property rights or copyright
- Using the trust's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the trust or academy 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
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the trust or its academies, or risks bringing the trust or its academies into disrepute
- Sharing confidential information about the trust or its academies, its pupils, or other members of the trust and its academy communities
- Connecting any device to the trust's or academies' ICT network without approval from authorised personnel

- Setting up any software, applications or web services on the trust or academies network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the trust or academies' ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the trust or its academies
- Using websites or mechanisms to bypass the trust's and its academies' filtering mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic 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 Academy Lead and Trust Executive Team will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the trust's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of trust ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Academy Lead's discretion.

In such cases you should seek approval from your Academy Lead who will inform the Director of Academy Operations. In cases involving the Central Team you should inform the Chief Finance Officer.

- 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

4.2 Sanctions

Pupils who engage in any of the unacceptable activity listed above may face disciplinary action in line with the academy behaviour policy. Staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the trust's disciplinary and dismissals policy, grievance policy, bullying and harassment policy or staff code of conduct.

Copies of these policies can be found on the trust website.

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

5.1 Access to school ICT facilities and materials

Bolton Impact Trust employs Schools ICT who manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

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

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

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact Schools ICT.

5.1.1 Use of email

The trust 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 trust has provided.

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

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

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

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

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

If you are sending the same email to more than one pupil/parent, email addresses should not be visible to other recipients as so to comply with GDPR. The use of BCC should be used under these circumstances.

If staff send an email in error that contains the personal information of another person, they must inform **Schools ICT and the Chief Finance Officer** immediately and follow our data breach procedure.

5.1.2 Use of Mobile Phones

Personal mobile phones

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

On occasions and in exceptional circumstances personal phones may need to be used for work purposes. In these instances approval should be sought from the Academy Lead and the withheld number facility should always be used. If approval cannot be sought prior to using a personal device staff must inform the academy lead as soon as possible after the use has taken place.

Full details regarding the use of personal mobile phones can be found in the academy mobile phone policy.

Work mobile phones

Sometimes it is necessary to provide staff with a work mobile phone to conduct work related business. All staff are required to read and sign the mobile phone declaration.

Any work mobile phones or devices, and all of its contents, remains the property of the Bolton Impact Trust along with any information contained or stored within the device. This should be considered retrievable and accessible at all times.

Mobile devices should only be used for work related business and not for personal use. You will be required to pay any costs incurred from the personal use of the device.

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

5.2 Personal use

Staff are permitted to occasionally use the trust ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Academy Lead may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

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

Staff may not use the trust'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 trust's ICT facilities for personal use may put personal communications within the scope of the trust'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 trust policies including; acceptable use policy, social media policy and staff code of conduct.

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

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

5.2.1 Personal social media accounts

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

The trust has guidelines for staff on appropriate security settings for Facebook accounts (see the social media policy).

5.3 Remote access

We allow staff to access the trust's ICT facilities and materials remotely. Remote access is via Citrix Remote Access and is managed by schools ICT. This uses the relevant academy network account along with 2 factor authentication for staff to login remotely. It provides a virtual desktop with access to the academy server and uses the same security access associated with internal login for restricting file access. We do not allow file transfer to remote computer or remote printing, so data remains on the academy server.

Staff accessing the trust'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 trust's ICT facilities outside of their academy and take precautions against viruses or compromising the 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. This policy can be found on the website and the school server.

5.4 School social media accounts

The trust has a number of official social media pages as detailed below:

Academy	Social media pages	Managed by/Posts by
Forwards Centre	Twitter	C Fielding
Youth Challenge	Twitter Facebook	V. Sutton, J.Higgins
Park School	Twitter Facebook	K. Hayes
Lever Park Lever Park Therapy Farm	Twitter Twitter	A Whitehead O. Fay
Executive Team	Twitter	P. Hodgkinson

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 can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times and complete the declaration form. (See social media policy for guidelines.)

5.5 Monitoring and filtering of academy networks 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 monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

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

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

The trust and its academies monitors ICT use in order to:

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

Our local governing bodies are responsible for making sure that:

- The school 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 academies monitoring and filtering systems

The academies designated safeguarding leads (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 academies DSL and ICT manager, as appropriate.

6. Pupils

6.1 Access to ICT facilities

Academy	Access to ICT
Forwards Centre	Computers and equipment are available to pupils only under the supervision of staff. Pupils will be provided with an account linked to the academy's virtual learning environment, which they can access from any device. If ICT equipment is loaned to pupils then a loan equipment form must be completed and co-signed by a member of staff. (See academy's remote learning policy for further detail.)
Youth Challenge	Computers and equipment 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 academies' virtual learning environment, which they can access from any device. If ICT equipment is loaned to pupils then a loan equipment form must be completed and co-signed by a member of staff. (See academy's remote learning policy for further detail.)
Park School	Computers and equipment 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 academies virtual learning environment, which they can access from any device. If ICT equipment is loaned to pupils then a loan equipment form must be completed and co-signed by a member of staff. (See academy's remote learning policy for further detail.)
Lever Park	Computers and equipment 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 academies virtual learning environment, which they can access from any device. If ICT equipment is loaned to pupils then a loan equipment form must be completed and co-signed by a member of staff. (See academy's remote learning policy for further detail.)

6.2 Search and deletion

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

Under the Education Act 2011, the headteacher/academy lead, and any member of staff authorised to do so by the headteacher/academy lead, 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 school rules as a banned item for which a search can be carried out **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 academy lead or designated safeguarding lead.
- 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

The authorised staff member should:

- Inform the Academy Lead or DSL of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item. A list of banned items is available the academy behaviour policy
- Involve the Academy Lead or DSL 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 school or disrupt teaching, **and/or**
- Commit an offence

If inappropriate material is found on the device, it is up to designated safeguarding lead or member of the 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 Academy Lead immediately, who will decide what to do next. The DSL/Academy Lead 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 / searches and confiscation policy
- Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the school complaints procedure.

6.3 Unacceptable use of ICT and the internet outside of school

The trust and its academies 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 school 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/trust policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual 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 trust or its academies, or risks bringing the trust or its academies into disrepute
- Sharing confidential information about the trust or its academies, other pupils, or other members of the trust/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 trust's ICT facilities
- Causing intentional damage to ICT facilities or materials

- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

7. Parents

7.1 Access to ICT facilities and materials

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

However, parents working for, or with, the trust or its academies in an official capacity (for instance, as a volunteer) may be granted an appropriate level of access, or be permitted to use the facilities at the Academy Lead's discretion.

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

7.2 Communicating with or about the academies/trust online

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

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

We ask parents to sign the agreement in appendix 2.

7.3 Communicating with parents/carers about pupil activity

The school 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 school pupils will be interacting with online, including the purpose of the interaction.

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

8. Data security

The trust 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 trust'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

8.1 Passwords

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

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

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

You will be required to update your password on a regular basis.

8.2 Software updates, firewalls, and anti-virus software

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

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

Any personal devices using the trust's networks must all be configured in this way.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the trust's data protection policy. This policy can be found on the website and on the school server.

8.4 Access to facilities and materials

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

These access rights are managed by schools ICT.

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 Academy Lead and schools ICT immediately.

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

8.5 Encryption

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

School staff may only use personal devices (including computers and USB drives) to access school 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 Academy Lead.

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

9. Protection from cyber attacks

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

The Trust and its academies will:

- Work with governors, trustees and Schools ICT 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'**: each academy will verify this using a third-party audit annually to objectively test that what it has in place is up to scratch
    - **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 academies and the trust needs to update its software
    - **Regularly reviewed and tested**: to make sure the systems are as up to scratch and secure as they can be
- Back up critical data. This will take place nightly and we will also keep weekly and monthly copies. Schools ICT will store these backups on [cloud based backup systems/external hard 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 (SIMS) to Schools ICT who will configure individual access that is role related as instructed by the Academy Lead or Trust Executive Team.
- We will delegate responsibility for maintaining the security of internal systems to the Academy/Central Leadership Team who will configure individual access.
- 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 school email accounts
    - Store passwords securely using a password manager
- Make sure Schools ICT conduct regular access reviews to make sure each user in the academies and the trust has the right level of permissions and admin rights
- Have a firewall in place that is switched on

- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and seeing if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the School's ICT department, for example, including how the academies or the trust will communicate with everyone if communications go down, who will be contacted when, and who will notify Action Fraud of the incident. This will be reviewed and tested annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
- Work with our trust board to see what it can offer regarding cyber security, such as advice on which service providers to use or assistance with procurement.

10. Internet access

The wireless internet connection, in each academy, is secured.

Sophos UTM firewalling and filtering protects the internet across the trust.
Internet access logging is to this local firewall and central servers.
Web content filtering are in place, this includes the IWF and Prevent watchlists for web filtering.
Data protection for Virus etc. is both via a local install of Sophos Endpoint (anti-virus) and gateway (UTM) scanning.
Filtering levels (access) is determined by Active Directory credentials – this is customised by each academy.
Server data protection is by Sophos (Intercept X) and data is backed up off site (Arcserve).
Server file access can be audited if required/requested, although as it is processor / memory intensive it is not turned on by default.
Access levels (permissions) are determined by Active Directory credentials given to individual users or groups.

Office 365 access is secured by the use of 2-factor authentication.
As per the server data, access levels (permissions) are determined by Active Directory credentials given to individual users or groups.
We do not have an offline backup service for O365, but use Microsoft's retention processes.

Although we use filtering across each of our academies, they are not fool proof. If you notice any inappropriate sites that the filters have not identified please inform schools ICT and your Academy Lead. If you notice any appropriate sites that have been filtered by mistake please also notify schools ICT.

10.1 Pupils

Pupils do not have access to Wi-Fi within any of our academies. If you are made aware of a pupil who has gained access to the Wi-Fi network, please inform your Academy Lead and schools ICT.

10.2 Parents and visitors

Parents and visitors to any of the academies will not be permitted to use the school's Wi-Fi unless the Academy Lead grants specific authorisation.

The Academy Lead will only grant authorisation if:

- Parents are working with the academy in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the academy's Wi-Fi 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 Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. Monitoring and review

The Academy Leads supported by the Executive Leadership Team and Schools ICT monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the trust and its academies.

This policy will be reviewed every 2 years.

11. Related policies

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

- Online safety Policy
- Safeguarding and child protection Policy
- Behaviour Policy
- Staff disciplinary Policy
- Staff Code of Conduct
- Grievance, Bullying and Harassment Policy
- Data protection Policy
- Remote learning Policy
- Mobile Phone Policy

Appendix 1: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our school. The academy uses the following channels: • Our official Facebook page • Email/text groups for parents (for school announcements and information) • Our virtual learning platform Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).	
When communicating with the academy/trust via official communication channels, or using private/independent channels to talk about the school, I will: • Be respectful towards members of staff, and the school, at all times • Be respectful of other parents/carers and children • Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure I will not: • Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way • Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident • Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers	
Signed:	**Date:**

Appendix 2: Acceptable use agreement for older pupils

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

Appendix 3: Acceptable use agreement for younger pupils

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

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

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 5: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber-attack and the measures the 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.
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.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.

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