The 3-18 Education Trust

ICT and Internet Acceptable Use Policy

'Every individual is in a great school.'

Approved: Spring Term 2025
Review: Spring Term 2026

www.3-18education.co.uk

Our Mission

To celebrate the diverse nature, culture and identity of our individual schools, whilst collaborating and enjoying the benefit of the team.

Our Values

Compassionate

To show care and understanding towards others.

Accomplished

To provide high quality education and training for all.

Resilient

To be solution focused and able to intelligently manage challenges.

The 3-18 Education Trust
101 Longden Road
Shrewsbury
SY3 9PS

Company Number: 08064698

Policy Monitoring and Review

Monitoring

The Chief Executive Officer will monitor the outcomes and impact of this policy on an annual basis.

Review

Member of Staff Responsible	Chief Executive Officer and IT Director
Relevant Guidance/Advice/Legal Reference	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 Education Act 2011 Freedom of Information Act 2000 Education and Inspections Act 2006 Keeping Children Safe in Education 2023 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
Policy Adopted By	Board of Trustees
Consultation	Local Governing Bodies
Date of Policy	Spring Term 2025
Review Period	Annually
Date of Next Review	Spring Term 2026

Contents

1. Introduction..... 6

2. Definitions 6
ICT Facilities 6
Users 6
Personal Use 6
Authorised Personnel 6
Materials 6
3. Unacceptable Use 7
Exceptions from Unacceptable Use 8
Sanctions 8
4. Staff (including trustees, local governors, volunteers, and contractors) 8
Access to Trust ICT Facilities and Materials 8
Use of Phones and Email 8
Personal Use 9
Personal social media accounts 10
Remote Access 10
Individual School Social Media Accounts 10
5. Pupils 11
Access to ICT Facilities 11
Search and Deletion 12
Unacceptable Use of ICT and the Internet Outside of School 13
6. Parents and Carers 14
Access to ICT facilities and materials 14
Communicating with or about the school online 14
Communicating with parents/carers about pupils' activities 14
7. Data Security 14
Passwords 15
Software updates, firewalls and anti-virus software 15
Data protection 15
Access to facilities and materials 15
Encryption 16
8. Protection from Cyber Attacks 16
9. Internet Access 17
Pupils 17
Parents, carers and visitors 17
10. Related Policies 17
Appendix 1: Social Media Cheat Sheet for Staff 19

Guide for staff on social media. 19
Appendix 2: Glossary of Cyber Security Terminology 22

1. Introduction

1.1. Information and communications technology (ICT) is an integral part of the way the 3-18 Education Trust (Trust) works, and is a critical resource for pupils, staff (including the senior leadership team), trustees and local governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school.

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

1.3. This policy aims to:

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

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

1.5. Breaches of this policy may be dealt with under the Trust's staff Code of Conduct and Disciplinary Policy and ach school's Behaviour Policy.

2. Definitions

ICT Facilities

2.1. 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 school's ICT service.

Users

2.2. Anyone authorised by the school to use the school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Personal Use

2.3. Any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user.

Authorised Personnel

2.4. Employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities

Materials

2.5. Files and data created using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

2.6. See Appendix 2 for a glossary of cyber security terminology.

3. Unacceptable Use

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

3.2. 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's or individual school'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 school into disrepute.
- Sharing confidential information about the school, its pupils, or other members of the school community.
- Connecting any device to the school's ICT network without approval from authorised personnel.
- Setting up any software, applications or web services on the school'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 school'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 school's ICT facilities.
- Causing intentional damage to the Trust's ICT facilities.
- Removing, deleting or disposing of the Trust'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 Trust or schools.
- Using websites or mechanisms to bypass the school'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 Copilot, 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.

3.3. This is not an exhaustive list. The Trust reserves the right to amend this list at any time. The Headteacher of each school or any other relevant member of Trust staff 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.

Exceptions from Unacceptable Use

3.4. Where the use of Trust ICT facilities (on Trust 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 Headteacher's discretion. Agreement must be sought prior to any activities and in writing.

3.5. Pupils may use AI tools and generative chatbots as a research tool to help pupils find out about new topics and ideas and when specifically studying and discussing AI in schoolwork, for example in IT lessons or art homework about AI-generated images, with the permission of a member of staff. All AI-generated content must be properly attributed.

Sanctions

3.6. Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the Trust and school's policies on pupil Behaviour, staff Code of Conduct and related policies.

3.7. Consequences of unacceptable use of Trust ICT can include a range of restrictions up to including the blocking of access to an individual's account.

4. Staff (including trustees, local governors, volunteers, and contractors)

Access to Trust ICT Facilities and Materials

4.1. The Trust manages access to the school's ICT facilities and materials for staff. That includes, but is not limited to:

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

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

4.3. 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 on-site technician or Trust IT Manager

4.4. Files and document libraries on SharePoint have an access request form available on SharePoint or can be requested by raising an IT support request/ ticket.

Use of Phones and Email

4.5. The Trust provides each member of staff with an email address. This email account should be used for Trust/work purposes only. Staff will have multi-factor authentication enabled on their email account(s).

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

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

4.8. 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.

4.9. 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.

4.10. 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.

4.11. 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.

4.12. If staff send an email in error that contains the personal information of another person, they must inform the IT Manager/their School Business Manager immediately and follow the Trust's Data Breach procedure.

4.13. Staff must not give their personal phone number(s) to parents/carers or pupils. Staff must use phones provided by the Trust to conduct all work-related business.

4.14. Trust phones must not be used for personal matters.

4.15. 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 in Unacceptable Use above.

4.16. The Trust has the ability to record incoming and outgoing phone conversations. All calls to the school office are recorded to aid administrators.

4.17. Staff who would like to record a phone conversation should speak to the IT Manager/their School Business Manager.

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

4.19. This could be when

- 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

4.20. Staff are permitted to occasionally use Trust ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The Trust IT Manger, Director or School Business Manager may withdraw or restrict this permission at any time and at their discretion.

4.21. Personal use is permitted provided that such use:

- Does not constitute ‘unacceptable use’, as defined in Unacceptable Use 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.

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

4.23. 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 Monitoring and Filtering of the Trust Network and Use of ICT Facilities below).

4.24. Where breaches of this policy are found, disciplinary action may be taken.

4.25. Staff should be aware that personal use of ICT (even when not using Trust 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.

4.26. Staff should read through the Guidelines for Facebook in Appendix 1 and apply these rules to social media generally.

Personal social media accounts

4.27. Members of staff should make sure 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 Appendix 1).

Remote Access

4.28. The Trust allows staff to access the Trust’s ICT facilities and materials remotely.

4.29. The Trust IT Support Team and the Trust’s third-party support partner manages the remote access system.

4.30. Staff will be required to use a personal device to verify their identity, if they wish to access school resources and student information outside of the Trust provided network.

4.31. Protocols for remote access

- Access must be for the shortest required amount of time required for the task.
- Access should only be on a staff equipment.
- Access should not be on any shared IT equipment, such as a family computer or Xbox, etc.

4.32. How staff can request remote access

- Staff accessing the school’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 school’s ICT facilities outside a Trust site and must take such precautions as the IT Manager may require against importing viruses or compromising system security.

4.33. The Trust’s 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 the Trust’s Data Protection Policy. This can be found on the Trust’s/school’s SharePoint site and the Trust’s/school’s website.

Individual School Social Media Accounts

4.34. Individual schools may have, from time to time, have official social media accounts, managed by authorised members of staff. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

4.35. Each school 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.

4.36. Monitoring and Filtering of the Trust Network and Use of ICT Facilities

4.37. 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.

4.38. Only authorised personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

4.39. The Trust monitors ICT use to

- Obtain information related to school business.
- Protect pupils online.
- Investigate compliance with school policies, procedures and standards.
- Ensure effective school 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.

4.40. The Board of Trustees is responsible for making sure that.

- The Trust 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.

4.41. Each of the Trust schools' Designated Safeguarding Lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

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

5. Pupils

Access to ICT Facilities

5.1. Computers and equipment in the school's ICT suite are available to pupils only under the supervision of staff.
5.2. Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff.
5.3. Sixth-form pupils can use the computers independently, for educational purposes only.

Search and Deletion

5.4. Under the Education Act 2011, the Headteacher, and any member of staff authorised to do so by the Headteacher, 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 (your behaviour policy should list these items), and/or
- Is evidence in relation to an offence.

5.5. 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)

5.6. 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 Headteacher / DSL.
- 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, the Headteacher / DSL should proceed according to the school's Behaviour Policy)

5.7. 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. A list of banned items is available is listed in individual school's Behaviour Policy.
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk.

5.8. 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.
5.9. 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

5.10. If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / Headteacher / 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.

5.11. 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.

5.12. 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.

5.13. 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.
- The individual school's Behaviour Policy.

5.14. Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the Trust's Complaints Policy.

Unacceptable Use of ICT and the Internet Outside of School

5.15. The school 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 bully or harass someone else, or to promote unlawful discrimination.
- Breaching the school'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 school, or risks bringing the school into disrepute.
- Sharing confidential information about the school, other pupils, or other members of the school 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 the Trust'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.

6. Parents and Carers

Access to ICT facilities and materials

6.1. Parents and carers do not have access to the Trust's ICT facilities as a matter of course. However, parents and carers working for, or with, the Trust or school 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 Trust's facilities at the Headteacher's discretion. Where parents and carers are granted access in this way, they must abide by this policy as it applies to staff.

Communicating with or about the school online

6.2. The Trust believes it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online. Parents and carers play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

Communicating with parents/carers about pupils' activities

6.3. 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 the school asks pupils to use websites or engage in online activity, the school 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.

7. Data Security

7.1. 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.

7.2. Staff, pupils, parents, carers and others who use the school's ICT facilities should use safe computing practices at all times. The Trust aims to meet the cyber security standards recommended by the DfE'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

7.3. All users of the Trust's ICT facilities should set strong passwords for their accounts and keep these passwords secure. Multi- factor authentication into accounts are required outside of the Trust's network. This may require users to use a personal device to prove identity.

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

7.5. 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

7.6. All of the Trust'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.

7.7. 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 school's ICT facilities.

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

Data protection

7.9. All personal data must be processed and stored in line with data protection regulations and the Trust's Data Protection Policy. This can be found on Trust/school SharePoint site and the Trust's/school's website.

Access to facilities and materials

7.10. 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 IT Director.

7.11. 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 on site IT support or Trust IT Manager immediately.

7.12. 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

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

7.14. 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 headteacher.

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

8. Protection from Cyber Attacks

8.1. Please see the glossary (Appendix 2) to help you understand cyber security terminology.

8.2. The Trust will:

- Work with trustees, local 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 Trust'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 the Trust's 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 Trust will at least annually verify this using a third-party audit (such as 360 degree safe) 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 the Trust's systems safe.
    - Up to date: with a system in place to monitor when the school 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 Barracuda servers.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to Arbor.
- Make sure staff:

    - Enable multi-factor authentication where they can, on things like school email accounts.
    - Store passwords securely using a password manager.
- Make sure IT Support Team staff conduct regular access reviews to make sure each user in 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 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 Trust 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 annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'.

9. Internet Access

9.1. The Trust's wireless internet connection is secure.

9.2. This managed at a Trust and school level:

- The Wi-Fi is filtered according to school network standards.
- Pupils are to use specific pupil Wi-Fi networks.
- Staff are to use the staff Wi-Fi for personal devices only.
- All school owned devices requiring Wi-Fi connectivity must be added to the network by a school IT technician or a Trust technician using the school Wi-Fi network.

Pupils

9.3. Pupils may access Wi-Fi at the discretion of the school and follow all policies and acceptable use rules.

Parents, carers and visitors

9.4. Parents, carers and visitors to the Trust will not be permitted to use the school's Wi-Fi unless specific authorisation is granted by the Headteacher.

9.5. The Headteacher will only grant authorisation if:

- Parents and carers are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school'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)
- Special events

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

10. Related Policies

This policy should be read alongside the Trust's and school's policies and documents on:
Safeguarding and Child Protection
Online safety
Behaviour
Staff Disciplinary
Data Protection
Data Breach Policy
Information Security Policy and Procedure
Filtering and Monitoring Policy
Acceptable Use Agreements

Appendix 1: Social Media Cheat Sheet for Staff

Do not accept friend requests from pupils on social media.

Guide for staff on social media.

- Make sure your profile image is not offensive in any way.
- Check your privacy settings regularly.
- Be careful about tagging other staff members in images or posts.
- Don't share anything publicly that you wouldn't be happy showing your pupils.
- Don't use social media sites during school hours.
- Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there.
- Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event).
- 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.
- Consider uninstalling the Facebook app from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi 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 – for Facebook 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 – for Facebook 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 headteacher 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 one parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers 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: Glossary of Cyber Security Terminology

These key terms will help to understand the common forms of cyber-attack and the measures the Trust have put in place.

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.
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.