St Chad's
Academies Trust

St Chad's
Academies Trust

Acceptable Use Policy

Children first; in the footsteps of St. Chad

As we follow Christ in the footsteps of St. Chad, we seek to be servant leaders who have a desire to see all those, within our Trust family, truly flourish both spiritually and academically.

Document title	Acceptable Use Policy		
Owner	Data Protection Officer		
Version	2.0	**Status**	FINAL
Approved on	21 August 2026	**Effective from**	01 September 2026
Last updated	11 August 2026	**Last updated by**	Lea Millinchip
Review date	01 September 2028		
Purpose	This policy outlines the acceptable and unacceptable use of the Trust's ICT resources, establishing expectations for online conduct to protect users from safeguarding and cyber security risks while maintaining compliance with relevant legislation.		
The policy has been implemented following consultation, in line with statutory practice, with central team colleagues and St Chad's Academies Trust Board, and may be amended from time to time, following further consultation with St Chad's Academies Trust Board			

Related Documents	St Chads Acceptable Use Policy St Chads Data Protection – A guide for colleagues St Chads Information and records retention policy St Chads Information security policy St Chads Privacy notices (Parents, Colleagues and pupils) St Chads Appropriate Policy Document
References	https://ico.org.uk/

If you would like this information in another language or format, please speak to the Trust.

Telephone: 01543 622 433

Contents

1. Introduction and Aims
2. Relevant legislation and guidance
3. Definitions
4. Unacceptable Use
5. Exceptions from unacceptable use
6. Sanctions
7. Colleagues (including LAC members, volunteers, and contractors) access to Academy Trust ICT facilities and materials.
8. Use of Phones and email
9. Personal Use
10. Personal social media accounts
11. Remote Access
12. Academy social media accounts
13. Monitoring and filtering of the school network and use of ICT facilities
14. Pupils access to ICT facilities
15. Search and Deletion
16. Unacceptable use of ICT and the internet outside of school
17. Parents/carers access to ICT facilities and materials
18. Communicating with or about the Academy Trust online
19. Communicating with parents/carers about pupil activity
20. Data security
21. Passwords
22. Software updates, firewalls and anti-virus software
23. Data protection
24. Access to facilities and materials
25. Encryption
26. Protection from cyber attacks
27. Monitoring and review

Appendix 1: Facebook cheat sheet for staff

Appendix 2: Glossary of cyber security terminology

Table of substantive changes from previous versions

This table explains where we have made substantive changes, for your ease of reference and assurance.

Date	Section Amended
11.08.2026	Document changed to Trust new policy format
11.08.2026	Section 2.1 amended to reference up to date link for Keeping children safe in education

1.0 Introduction and aims

1.1 St Chad's Academies Trust ('the Trust') is committed to ensuring that it provides a strong infrastructure to enable our academies to flourish and improve. The Trust recognises that its leaders and colleagues are central to this success and greatly values their commitment and contribution.

1.2 The core values of the Trust form the basis of all discussions with colleagues. We expect all colleagues of St. Chad's Academies Trust to respect and model these values

1.3 St Chad's Academies Trust and its academies are referred to in this policy as the A**cademy Trust** or **we**.

1.4 Information and communications technology (ICT) is an integral part of the way our Academy Trust works, and is a critical resource for pupils, colleagues (including the senior leadership team), local academy committee members (LAC), volunteers and visitors.

1.5 The ICT resources and facilities our academies use could also pose risks to data protection, online safety, and safeguarding.

1.6 This policy aims to:

1.6.1 Set guidelines and rules on the use of the Academy Trust ICT resources for colleagues, pupils, parents/carers, local academy committees and trustees.

1.6.2 Establish clear expectations for the way all members of the Academy Trust community engage with each other online.

1.6.3 Support the Academy Trust policies on data protection, online safety, and safeguarding

1.6.4 Prevent disruption that could occur to the Academy Trust through the misuse, or attempted misuse, of ICT systems.

1.6.5 Support the school in teaching pupils safe and effective internet and ICT use

1.7 This policy covers all users of our Academy Trusts ICT facilities, including LAC members, colleagues, pupils, volunteers, contractors, and visitors.

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

2.0 Relevant legislation and guidance

2.1 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

Education and Inspections Act 2006

https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

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

3.0 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 Academy Trust ICT service.

Users: anyone authorised by the Academy Trust to use the ICT facilities, including Local academy committee members, colleagues, 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: colleagues authorised by the Academy Trust to perform systems administration and/or monitoring of the ICT facilities.

Materials: files and data created using the Academy Trust ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

3.1 See appendix 2 for a glossary of cyber security terminology.

4.0 Unacceptable use

4.1 The following is considered unacceptable use of the Academy Trust ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings.

Unacceptable use of the Academy Trusts ICT facilities includes:

- Using the academy ICT facilities to breach intellectual property rights or copyright
- Using the academy ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the 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 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 Academy Trust, or risks bringing the academy into disrepute
- Sharing confidential information about the Academy Trust, its pupils, or other members of the school community
- Connecting any device to the Academy Trust ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the Academy Trust 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 Trust 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 Trust ICT facilities
- Causing intentional damage to the Academy Trust ICT facilities

- Removing, deleting or disposing of the Academy Trust 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 Trust
- Using websites or mechanisms to bypass the Academy Trust filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

4.2 This is not an exhaustive list. The Academy Trust reserves the right to amend this list at any time.

4.3 Authorised colleagues will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the Academy Trust ICT facilities.

5.0 Exceptions from unacceptable use

5.1 Where the use of the Academy Trust ICT facilities (on the 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 executive/principal's discretion.

6.0 Sanctions

6.1 Pupils and colleagues who engage in any of the unacceptable activities listed above may face disciplinary action in line with the Academy Trusts policies on behaviour/discipline/staff discipline/staff code of conduct.

7.0 Colleagues (including LAC members, volunteers, and contractors) access to Academy Trust ICT facilities and materials

7.1 The Academy Trusts network providers, school business manager (SBM) and principals manage access to the Academy Trust ICT facilities and materials for academy colleagues. That includes, but is not limited to:

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

7.2 Colleagues will be provided with unique login/account information and passwords that they must use when accessing the Academy Trust ICT facilities.

7.3 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 network providers, school business manager (SBM) or principal.

8.0 Use of phones and email

8.1 The Academy Trust provides each colleague with an email address.

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

8.3 All work-related business should be conducted using the email address the Academy Trust has provided.

8.4 Colleagues 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.

8.5 Colleagues 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.

8.6 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.

8.7 Colleagues 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.

8.8 If colleagues 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.

8.9 If colleagues send an email in error that contains the personal information of another person, they **MUST** inform the Data Protection Officer (DPO) and follow our data breach procedure.

8.10 Colleagues must not give their personal phone number(s) to parents/carers or pupils. Phones provided by the academy should be used to conduct all work-related business.

8.11 Academy phones must not be used for personal matters.

8.12 Colleagues 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 section 4.

9.0 Personal use

9.1 Staff are permitted to occasionally use Academy Trust ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The executive/ principal may withdraw or restrict this permission at any time and at their discretion.

9.2 Personal use is permitted provided that such use:

- Does not take place during the operational academy day.
- 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 colleagues or pupils from using the facilities for work or educational purposes

9.3 Colleagues may not use the Academy Trust ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos.

9.4 Colleagues should be aware that use of the Academy Trust ICT facilities for personal use may put personal communications within the scope of the Academy Trust ICT monitoring activities (see section 4). Where breaches of this policy are found, disciplinary action may be taken.

9.5 Colleagues are also permitted to use their personal devices (such as mobile phones or tablets) in line with the academy mobile phone/personal device policy.

9.6 Colleagues should be aware that personal use of ICT (even when not using school 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.

9.7 Colleagues should take care to follow the school's guidelines on use of social media (see appendix 1) and use of email (see section 8) to protect themselves online and avoid compromising their professional integrity.

10.0 Personal social media accounts

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

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

11.0 Remote access

11.1 We allow colleagues to access the school's ICT facilities and materials remotely.

11.2 Remote access must be agreed with the academy executive/principal, SBM or IT provider.

11.3 Colleagues accessing the Academy Trust ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Colleagues must be particularly vigilant if they use the Academy Trust ICT facilities outside the academy and must take such precautions as the network provider, SBM or executive/principal may require against importing viruses or compromising system security.

11.4 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.

12.0 Academy social media accounts

12.1 The Academy Trust has official Facebook, X, LinkedIn, and YouTube accounts, managed by authorised colleagues. Colleagues who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

12.2 The Academy 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.

13.0 Monitoring and filtering of the school network and use of ICT facilities

13.1 To safeguard and promote the welfare of children and provide them with a safe environment to learn, the Academy 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

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

13.3 The school monitors ICT use in order to:

- Obtain information related to school business
- 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

13.4 The Local Academy Committees LACs are responsible for making sure that:

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

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

13.6 Where appropriate, colleagues may raise concerns about monitored activity with the academy trusts DSL and DPO, as appropriate.

14.0 Pupils access to ICT facilities

14.1 Computers and equipment in the academy ICT suites are available to pupils only under the supervision of colleagues".

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

14.3 Pupils will be provided with an account linked to the academy virtual learning environment, which they can access from any device.

15.0 Search and deletion

15.1 Under the Education Act 2011, the executive-/principal, and any colleague authorised to do so by the executive-/principal, can search pupils and confiscate their mobile phones, computers or other devices that the authorised colleague has reasonable grounds for suspecting:

- Poses a risk to colleagues or pupils, and/or
- Is identified in the academy 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)

15.2 Before a search, if the authorised colleague 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 colleagues. If the search is not urgent, they will seek advice from the executive / principal 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.

15.3 The authorised colleague 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 in the academy behaviour policy.
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

- Authorised colleagues 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.

15.4 When deciding whether there is a 'good reason' to examine data or files on a device, the colleague 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

15.5 If inappropriate material is found on the device, it is up to the colleague, in conjunction with the DSL and Executive-/principal to decide on a suitable response. If there are images, data or files on the device that are reasonably suspected are likely to put a person at risk, they will first consider the appropriate safeguarding response.

15.6 When deciding whether there is a good reason to erase data or files from a device, colleagues 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, colleagues 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

15.7 If a colleague 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

15.8 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
- Academy behaviour policies - searches and confiscation.

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

16.0 Unacceptable use of ICT and the internet outside of school

16.1 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 Trust 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 Trust, or risks bringing the trust into disrepute
- Sharing confidential information about the Academy Trust, 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 Trust ICT facilities
- Causing intentional damage to the Academy Trust 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

17.0 Parents/carers access to ICT facilities and materials

17.1 Parents/carers do not have access to the Academy Trust ICT facilities as a matter of course.

17.2 However, parents/carers working for, or with, the Academy Trust in an official capacity (for instance, as a volunteer or as a member of the PTFA may be granted an appropriate level of access or be permitted to use the Academy Trust facilities at the executive/principal's discretion.

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

18.0 Communicating with or about the Academy Trust online

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

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

19.0 Communicating with parents/carers about pupil activity

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

19.2 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.

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

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

20.0 Data security

20.1 The Academy Trust is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, colleagues 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 cybercrime technologies.

20.2 Colleagues, pupils, parents/carers, and others who use the Academy Trust 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

21.0 Passwords

21.1 All users of the Academy Trust ICT facilities should set strong passwords for their accounts and keep these passwords secure.

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

21.3 Colleagues 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.

21.4 All colleagues are advised to use password manager to help them store their passwords securely. Teachers will generate passwords for pupils using the required password manager or generator and keep these in a secure location in case pupils lose or forget their passwords.

22.0 Software updates, firewalls and anti-virus software

22.1 All of the Academy Trust 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.

22.2 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 Trusts ICT facilities.

22.3 Any personal devices using the Academy Trust network must all be configured in this way.

23.0 Data protection

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

24.0 Access to facilities and materials

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

24.2 These access rights are managed by the ICT provider, SBM or executive/principal.

24.3 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 Executive/principal immediately.

24.4 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.

25.0 Encryption

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

25.2 Colleagues may only use personal devices (including computers and USB drives) to access academy trust data, work remotely, or take personal data (such as pupil information) out of an academy if they have been specifically authorised to do so by the executive/principal.

25.3 Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the ICT provider, SBM or executive/principal.

26.0 Protection from cyber attacks

Please see the glossary (appendix 6) to help you understand cyber security terminology.

The Academy Trust will:

- Work with Trustees and the IT provider to make sure cyber security is given the time and resources it needs to make the Academy Trust secure

- Provide annual training for colleagues and include this training in any induction for new starters, 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 colleagues 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 Trust will 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 our systems safe

  Up to date: with a system in place to monitor when the Academy Trust 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 and store these backups on cloud-based backup systems that aren't connected to the Academy Trust network and which can be stored off the Academy Trust premises.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our cloud-based provider.
- 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

- Make sure ICT providers conduct regular access reviews to make sure each user in the Academy 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 Academy 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'

27.0 Monitoring and review

27.1 The Trust compliance officer monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the Academy Trust.

27.2 This policy will be reviewed every 2 years, unless there are significant changes in legislation/regulation which require an earlier review.

Appendix 1: Facebook cheat sheet for staff

Do not accept friend requests from pupils on social media

10 rules for school 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, our school or your pupils online – once it's out there, it's out there
8. 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)
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 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** – 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 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 colleague, 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 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.

TERM	DEFINITION
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.

TERM	DEFINITION
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.