# E-Safety and ICT Acceptable Use Policy

| | | | | |
|---|---|---|---|---|
| Policy Version Number: | 2 | | | |
| This policy applies to : | All members of the PLT community, including students, staff, parents/carers, governors/trustees, contractors, volunteers and visitors | | | |
| Related Documents/ Policies: | Data Protection Policy<br>Disciplinary Policy<br>Safeguarding Policy (Academy)<br>Student Behaviour Policy (Academy)<br>Staff Code of Conduct<br>Filtering and Monitoring Strategy | | | |
| Author: | Pamela McIlroy | | | |
| Area: | L&M | | | |
| Changes made/Reason for Review: | Reviewed and updated (combined with E-Safety Guidance) | | | |
| Approval required by (please tick): | A&R ✔ | F&R | Trust ✔ | Rem |
| Agreed by /Date: | TET/SLT (All Academies) | | | |
| Consultation with/date | LJC/JCNC (if applicable) | | n/a | |
| Approved by/Date | A&R | | 5/3/2024 | |
| Ratified by/Date | Trust Board | | 12/3/2024 | |
| Date of Next Review: | March 2027 | | | |
| Equality Impact Assessment | This Policy has been reviewed against equal opportunities legislation with regard to age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marriage and civil partnership and pregnancy and maternity and has no identified adverse impact (direct or indirect) on minority groups. | | | |

**Contents**



## 1. INTRODUCTION

ICT is an integral part of the way our Trust works, and is a critical resource for students, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the academies in the Trust.

We encourage the use of technology in order to enhance skills and promote achievement. However, the accessible and global nature of the internet and variety of technologies available mean that we have to be vigilant in the face of potential risks and challenges associated with such use, these include online safety and safeguarding and risks to data protection and the Trust's networks. The

term ‘e-safety’ is used to encompass the safe use of online technologies in order to protect pupils and staff from known and potential risks.

This policy aims to:

- Set guidelines and rules on the use of ICT resources for staff, students, parents and governors
- Establish clear expectations for the way all members of the Trust community engage with each other online
- Support the Trust’s policy on data protection, online safety and safeguarding
- Prevent disruption to the Trust through the misuse, or attempted misuse, of ICT systems
- Establish a framework for teaching students safe and effective internet and ICT use.

Breaches of this policy may be dealt with under our staff disciplinary policy/student behaviour policy. Where necessary, inappropriate activity will be reported to relevant external agencies.

The academies have additional guidance in place for the delivery of online learning where classes are held remotely during any period of academy closure.

## 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
- 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

## 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 to use the ICT facilities, including governors, staff, students, 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 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
**"Academy":** any member institution that is part of The Pinnacle Learning Trust
**"Cyber-bullying":** takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.
**"Phases"** phases of education, eg Primary, Secondary, Sixth Form

NB The term 'student' is used throughout this document to refer to pupils and students in all phases.

## 4. ACCESS TO ICT FACILITIES AND MATERIALS

All users of the academy's ICT facilities will have clearly defined access rights to academy systems, files and devices. These access rights are managed by the Trust Deputy Head of IT Services, or delegated person at each academy.

Users are provided with unique log-in/account information and passwords that they must use when accessing the academy's ICT facilities. It is their responsibility to keep their log in details secure. It is a breach of this policy for a user to share their log-in details with anyone else and this may result in disciplinary action.

Users should enable multi-factor authentication on their email account(s) and other Trust systems, as required.

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 a member of the IT Services team immediately.

The Data Protection Policy should be adhered to at all times when accessing the Trust's networks. 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.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access.

Staff and students may be loaned a mobile device (eg Chromebook or Laptop) for use in and outside of school/college, for their use only. Users should not allow anyone else access to their device and/or academy systems/data.

Staff and students must not install software to academy's ICT facilities, this includes devices issued for working remotely such as laptops/chromebooks, without authorisation from the Head of IT Services.

### 4.1. Remote access

We allow staff and students (depending on need) to access the academy's ICT facilities and materials remotely.

Users accessing the academy's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Users must be particularly vigilant if they use the academy's ICT facilities outside the academy and take such precautions as required to protect against importing viruses or compromising system or data security.

## 5. FILTERING AND MONITORING

The Trust has a Filtering and Monitoring Strategy in place to ensure that our academies meet the DfE's filtering and monitoring standards and ensure compliance with academy and Trust policies, procedures and standards. The Filtering and Monitoring strategy provides information on staff responsibilities, including how to report concerns, and how they will be dealt with.

Staff and students should be aware that the Trust monitors activity on its ICT facilities in order to provide a safe environment for children and young people. Inappropriate activity (even personal communication) will be reported to the DSL and/or Principal, which may result in disciplinary action.

## 6. UNACCEPTABLE USE

The following is considered unacceptable use of the Trust's ICT facilities (equipment, network or wifi) by any member of our Trust community, whether on or off Trust premises. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 5.2 below).
Unacceptable use of ICT facilities includes:

- Breaching the academy or Trust's policies or procedures
- Using the academy's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- 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
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- Using inappropriate or offensive language
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Activity which defames or disparages the academy or Trust, or risks bringing the Trust into disrepute

- Sharing confidential information about the academy or Trust, its students, or other members of its community
- Connecting any device to the academy's ICT network without approval from authorised personnel
- Using the academy's ICT facilities to breach intellectual property rights or copyright
- Setting up any software, applications or web services on the academy's 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 academy's 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
- Promoting a private business, unless that business is directly related to the academy or Trust
- Using websites or mechanisms to bypass the academy's filtering or monitoring mechanisms
- 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's senior leadership team will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the academy's ICT facilities.

### 6.1. Exceptions

Where the use of ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Principal's discretion. Where teachers feel that exemptions would support learning (for example, researching a topic that would usually be blocked through filtering), this should be agreed with Senior Leaders and/or the line manager of the teacher.

### 6.2. Sanctions

Students and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the academy's Behaviour policies for students and the Trust's Disciplinary Policy for staff.

Students may be disabled from the network for a specific period until an investigation has taken place or until such time that the Principal (or other member of SLT) determines appropriate.

## 7. STUDENTS

## 7.1. Educating Children and Young People about Online Safety

ICT and online resources are increasingly used across the curriculum. We believe it is essential for Online Safety guidance to be given to students on a regular and meaningful basis (dependent on age).

As part of the statutory relationships and health education in primary schools and relationships, sex and health education in secondary schools, students are taught about online safety and harms. Online Safety is embedded within our curriculum, particularly in PSHE/Citizenship/Tutorial and Computing and we continually look for new opportunities to promote Online Safety.

We provide opportunities within a range of curriculum areas to teach about Online Safety. Educating children and young people on the dangers of technologies that may be encountered outside of the academy is done informally when opportunities arise and as part of the curriculum. Through this curriculum, students become aware of the relevant legislation when using the internet, such as data protection and intellectual property which may limit what they want to do but also serves to protect them.

- Students are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities
- Students are taught about keeping their personal data safe and secure
- Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline
- Students are taught to critically evaluate materials (to be aware of clickbait and fake news) and learn good searching skills.
- Students are taught to be mindful of their digital footprint and be mindful of what they post online, aas well as reviewing their privacy settings regularly.

## 7.2. Examining Electronic Devices

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the Principal, or other authorised member of staff, has the right to search and confiscate students' phones, computers or other devices if they have reasonable grounds for suspecting they contain data, text or images banned under academy rules or legislation.

If inappropriate material is found on the device, it is up to the DSL, Principal or senior leader 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.

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 the academy's rules. Devices containing material which may constitute evidence relating to a suspected offence will be handed over to the police. If a staff member **suspects** a device **may** contain an indecent image of a child, 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.

Students refusing to hand over equipment following a request from a member of staff, will be dealt with through the academy's behaviour policy.

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

### 7.3. Email

The use of email is an essential means of communication in some of our academies and students will be provided with an academy email address (depending on the age of students). Where email accounts are provided, they will be restricted for internal use only, apart from sixth form students who will also be able to send external emails. Students are expected to comply with the conditions in this policy when using email and to adhere to the generally accepted rules, particularly in relation to the use of appropriate language, not revealing any personal details about themselves or others. Students should be aware of the potential risks involved in clicking on links and opening attachments (eg Phishing). Academy email addresses should be used for academy related business only.

### 7.4. Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others.

We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim. The academy will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. This will be discussed in class and within assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, Trustees and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training.

The academy also shares information with parents/carers via the academy website so that they are aware of the signs, how to report it and how they can support children and young people who may be affected.

In relation to a specific incident of cyber-bullying, the academy will follow the processes set out in the academy behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the academy will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

### 7.5. Use of AI

Students' use of AI must comply with the Academy's Student Code of Conduct for use of AI (where applicable).

## 8. STAFF (including governors, volunteers, and contractors)

### 8.1. Use of email and phones

The academy provides each member of staff with an email address. This email account should be used for work purposes only. All work-related business should be conducted using the email address the academy has provided, or via Google Classroom (where applicable). All contact with students must be for legitimate reasons.

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 using Egress (or other encryption software) so that the information is only accessible by the intended recipient. If staff send an email in error which contains the personal information of another person, they must inform the Data Protection Officer immediately and follow the data breach procedure.

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.

The Trust Code of Conduct states that staff must not disclose their personal phone numbers and/or email addresses to students or their parents. Staff must use phones provided by the Trust to conduct all work-related business where possible. 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 section 4.

### 8.2. Personal use of Trust ICT facilities

Staff are permitted to occasionally use academy ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Principal or Head of IT Services 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 students are present

- Does not interfere with their jobs, or prevent other staff or students from using the facilities for work or educational purposes

Staff are permitted to use their personal devices (such as mobile phones or tablets) to access Trust networks in line with this policy.

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

### 8.3. Social Media Accounts

The Trust and its academies have official social media pages, managed by designated members of staff. Social Media accounts using the Pinnacle Learning Trust (or any of its academies or sub-brands) name or logo must be approved by the Trust Marketing Manager or Academy Principal. Content on these accounts should be professional and reflect well on the Trust. Links to external sites must be appropriate and safe.

Those who are authorised to manage official social media accounts must ensure they abide by the guidelines in section 6 at all times.

Staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times. Anything staff post or publish on the internet or on any social networking site, relating to the Trust, their colleagues, parents or students/students must be respectful and not cause offence or detriment to those concerned. If in doubt, don't post. Staff may like, share or make appropriate comments in response to the Trust's official social media accounts.

In addition the use of images of staff, students and members of the public must follow the guidelines in the Trust's Data Protection Policy.

Further guidance can be found in Appendix 1.

## 9. PARENTS AND CARERS

We believe it is important to model for students and help them 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 academy via email or through our website and social media channels.

### 9.1. Access to ICT facilities and materials

Parents do not have access to the academy's ICT facilities as a matter of course. However, parents may have access to the academy's on-line systems to access information about their child, and in accessing these systems must abide by the principles of this policy.

Parents working for, or with, the academy in an official capacity (for instance, as a volunteer) may be granted an appropriate level of access, or be permitted to use the academy's facilities at the Principal's discretion. Where parents are granted access in this way, they must abide by this policy as it applies to staff.

### 9.2. Keeping Parents and Carers Informed about Online Safety

The academy will raise parents' and carers' awareness of internet safety in letters or other communications home, and in information via their website or text messaging service. This policy will be shared with parents via the academy website.
Online safety may also be covered during parents' evenings and specific sessions as required by individual academies.
If parents or carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL.
Concerns or queries about this policy can be raised with any member of staff or the Principal.

**PARENTAL INVOLVEMENT**
We believe that it is essential for parents/ carers to be fully involved with promoting online safety both in and outside of academy and also to be aware of their responsibilities.
Academies will regularly consult and discuss Online Safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.
Parents/ carers are asked to read through and agree to the acceptable use policy on behalf of their child on admission to academy (for under 16s).
Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g., on academy website).

Academies may disseminates information to parents relating to Online Safety by:

- Information and celebration evenings
- Posters
- Website postings/social media
- Newsletter items
- Special online safety events
- Email/parent apps

## 10. GUEST ACCESS

Visitors to the academy may be permitted to use the academy's wifi using the Guess WiFi password. Visitors who need to access the academy's wifi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan) can request access to the Guest Wifi services. Anyone using this facility must abide by the principles of this policy.

Staff must not give the wifi password to anyone who is not authorised to have it.

## 11. SYSTEM/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 ICT resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.

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
- Multi-factor authentication

Staff, students, parents/carers and others who use the academy's ICT facilities should use safe computing practices at all times. Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the academy's ICT facilities. Users should report any incidents of suspicious activity (including suspected unauthorised access, phishing attempts or cyber security issues) to the Head of IT Services/MIS immediately.

The Trust will not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data.

The Trust has a Data Protection Policy in place.

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

### 11.1. Encryption

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

Staff should use academy devices to access academy systems and data. Where a personal device is used, eg mobile phone or tablet, to access academy data, work remotely, or take personal data (such as student information) out of the academy, they should ensure the security of the device and encryption of data in accordance with this policy and the Data Protection Policy. The use of USBs is not allowed.

## 12. ROLES AND RESPONSIBILITIES

### 12.1. Designated Safeguarding Lead (DSL):

The DSL takes lead responsibility for online safety in the academy, in particular:

- Working alongside SLT colleagues, IT Services Manager, MIS Manager Trust Head of IT Services and other staff as necessary to ensure the Filtering and Monitoring Strategy is effective and address any online safety issues
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy and the Filtering and Monitoring Strategy.
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the Academy's behaviour policy.

- Where any report of an e-safety incident is made, all parties should know what procedure is triggered and how this will be followed up. Where it is considered appropriate, the safeguarding team will involve additional support from external agencies
- Updating and delivering staff training on online safety as appropriate and in conjunction with staff development needs.
- Ensure students are aware of online dangers and concerns, and use a variety of age appropriate methods to get this message across.
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in the academy to the Principal and/or governing board as requested.

### 12.2. Trust Head of IT Services/MIS:

The Trust Head of IT Services/MIS is responsible for:

- Putting in place and maintaining appropriate filtering and monitoring systems, in line with the Filtering and Monitoring Strategy, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content, including terrorist and extremist material (See Prevent Risk Assessment and Action Plan)
- Ensuring that the Trust's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- monitoring, together with the academy Principal, the implementation of this policy
- Reviewing and updating this policy to ensure that it reflects the needs and circumstances of the Trust/academy.

### 12.3. Staff:

All staff, including contractors and agency staff and volunteers, are responsible for:

- Understanding and implementing this policy in relation to their use of mobile devices, laptops, and through their remote learning environment where good practice must be actively promoted
- Agreeing and adhering to the terms on acceptable use of the academy's IT systems and the internet and ensuring that students follow the terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Reporting any concerns immediately to the DSL
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Academy Behaviour Policy
- Completing e-safety and cyber essentials training when prompted, and to read through and adhere to e-safety guidance relating to remote and online learning when issued. See also 'Safer Use of Electronic Media – Guidance for Staff' (Appendix 1).
- Keep passwords secure and report any suspected unauthorised access, phishing attempts, or cyber security issues to the Head of IT Services/MIS immediately.

Staff will accept the conditions of this policy when they log into a trust network and when they sign the Staff Code of Conduct.

### 12.4. Students:

- Students are responsible for using the Academy IT systems and mobile devices in accordance with this policy. They are required to accept the conditions of this policy by:
    - confirming on logging into the network; or
    - signing an acceptable use agreement when joining the academy; or
    - their parents signing an acceptable use agreement when their child joins the academy.
- Students must know what to do if they have e-safety concerns and who to talk to. In most cases, this will be their class teacher, academy staff and/or the safeguarding/additional support team.

**APPENDIX 1 SAFER USE OF ELECTRONIC MEDIA – GUIDANCE FOR STAFF**

**INTRODUCTION**

1.1 Pinnacle Learning Trust recognises the benefits and opportunities which new technologies offer to teaching and learning. We encourage the use of technology in order to enhance skills and promote achievement, and staff should feel that they can use electronic media such as social networking sites to communicate with others. It is essential, however, that you take care with the information you make public and remember that once a comment or posting is made, it may not be possible to take it back; there will always be a permanent digital record of it.

1.2 As a Trust employee, you should remember your public role and always consider how your conduct both online and more generally could affect your professional reputation and the reputation of your employer.

1.3 This guidance is intended to give you a number of simple hints to assist you to keep your information safe when using electronic media and to protect you from putting yourself and your employment at risk.

**SOCIAL NETWORKING AND SOCIAL MEDIA**

2.1 Social networking encourages communication and the sharing of information. Social networking websites are used regularly by millions of people and focus on building online communities of people who share interests and/or activities or who are interested in exploring the interests and activities of others.

2.2 The most popular social networking sites are Facebook, X, formerly known as Twitter, Instagram, Snapchat and TikTok: USING FACEBOOK, TWITTER, INSTAGRAM, SNAPCHAT, TIKTOK (and other popular platforms)

In order to stay safe, you should:

● Create separate ‘professional’ and ‘personal’ profiles and use them accordingly;

● Keep your professional and personal life separate – it is not acceptable for employees to make or accept friend requests (or similar) on social media platforms from current students and inadvisable for staff to make or accept such requests from former students;

● Remember your role as a member of staff and that you should always consider how your conduct could affect your professional reputation and the reputation of the academy;

● Set your social networking profile to private so that only your chosen friends can see any photos you publish on it; ● Think before you post any photos of yourself (or comments) on the Internet - ask yourself if you would be comfortable with others such as your colleagues, manager, students, their parents, etc seeing them;

● Make sure that you use a strong password with a combination of numbers and letters and that you keep this password safe. If you use a public or shared computer to access your social networking site (outside of academy), cancel any auto-login or ‘remember me’ functions and always make sure you log out at the end of the session. This will prevent anyone from accessing your account.

**MICROBLOGGING ADVICE**

3.1 X, formerly known as Twitter, is a free social networking and microblogging service that enables users to send and read messages known as tweets. Tweets are text-based posts displayed on the author's profile page and delivered to the author's subscribers who are known as followers. Senders can restrict delivery to those in their circle of friends or, by default, allow open access.

3.2 In order to stay safe when using X, you should:

● Check who is following you. This will enable you to block anyone you do not wish to see your "tweets” (updates). Once you've logged in, X shows your home page. Click on "followers” in the upper right-hand menu. There you'll see a list of everyone who has subscribed to be updated whenever you post something. You have three options for each follower: You can click their picture to see their own X page; you can choose to follow them as well; or you can block them from seeing your updates or "tweets”. You may want to block colleagues and students, etc from seeing your updates if you are posting personal items.

● Set your privacy settings: Again, this will limit who sees your updates and also enable you to change your username so it is not your actual name. In the top right sidebar menu on X there is an item called "settings." Go here to control what others can find out about you.
● Pick a username that's not your actual name: Your user name is also the URL that Xgives you and the name all your tweets are posted under. To separate your work life from your home life, choose something that affords you some degree of anonymity on Xbut also remember to choose something appropriate. You could create two separate accounts one for professional use and the other for personal allowing this separation to take place.
● Your profile picture: If you don't want colleagues or students to follow you on X, you might not want to put up your own photo. Consider using a graphic or some sort of icon. If you do want to be recognised, consider not posting anything that shows you in a way that you wouldn't want to appear if you were actually standing in the classroom.
● Don't talk about work in your "One Line Bio": Twitter offers a one-line biography of limited length to describe yourself. Consider mentioning your hobbies or other interests instead of your job title or where you work.

**HOW DO I GET OFFENSIVE CONTENT TAKEN DOWN?**
4.1 If upsetting or inappropriate images or information is found on the Internet the first person to contact is the person who is responsible for posting the material. If this is not possible then you can contact the service providers and request the information to be removed.
4.2 The following contact details will help you in the event that you discover any comments or postings which you consider to be offensive:
FACEBOOK – Reports can be made by clicking on the 'Report' link located on pages throughout the site, or by email to abuse@facebook.com or www.facebook.com/safety
TIKTOK - Reports can be made by clicking 'report' on the relvant category - https://support.tiktok.com/en/safety-hc/report-a-problem
TWITTER – To report violations of privacy or threatening behaviour guidelines are published on https://help.twitter.com/en/rules-and-policies/x-report-violation
INSTAGRAM – Reports can be made by clicking on Report Inappropriate and following the link for spam, scam or abusive content. Follow this link for more information https://help.instagram.com/547601325292351?helpref=search
SNAPCHAT - Reports can be made by following this link https://support.snapchat.com/en-GB/a/report-abuse-in-app TIKTOK - To report inappropriate content follow the guidance on this page https://support.tiktok.com/en/safety-hc/report-a-problem
YouTube – Logged in YouTube members can report inappropriate content by using the 'flag content as inappropriate' function which appears under every video. http://icanhaz.com/YouTubeSafety.com

**TikTok**
According to TikTok, the app is intended for users aged 13 and over. TikTok has a support centre with FAQs on the topic of age restrictions and privacy. If you learn that your child under the age of 13 has registered for a TikTok account, you can contact them at: https://www.tiktok.com/legal/report/privacy

If students are using TikTok at the academy, and they are under the age of 13, notify the e-safety/safeguarding lead at your academy. In addition, if students of any age are filming videos of your lessons, or you are aware they are filming other teachers, you will need to follow the behaviour management policy at your academy.

On TikTok, users can control who can see their uploaded content, follow them, and send them messages by making their account private. With a private account, users can approve or deny followers and restrict their uploaded content and incoming messages to followers only. If a user has a public profile, anyone signed into the TikTok app can view that user's public videos. However, only approved followers can send that user a message.

Whether users choose to have a public or a private account, they can always:

- Block another from contacting them at any time
- Save a video privately so that content will not be viewable by any other user
- Even with a private account, profile information – including profile photo, username, and bio – will be visible to all users.

So you will need to be careful about the information you disclose on your profile information.

### 10 rules for academy 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 students
6. Don't use social media sites during academy hours
7. Don't make comments about your job, your colleagues, our academy or your students online – once it's out there, it's out there
8. Don't associate yourself with the academy on your profile (e.g. by setting it as your workplace, or by 'checking in' at a academy 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 students)

---

### Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, students 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 student adds you on social media**

- In the first instance, ignore and delete the request. Block the student from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the student asks you about the friend request in person, tell them that you're not allowed to accept friend requests from students and that if they persist, you'll have to notify senior leadership and/or their parents/carers. If the student 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 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the academy
    - students 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 student 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: Acceptable use agreement for older students

<table>
<tr><th colspan="2">Acceptable use of the academy's ICT facilities and internet: agreement for students and parents/carers</th></tr>
<tr><td colspan="2">Name of student:</td></tr>
<tr><td colspan="2">When using the academy's ICT facilities and accessing the internet in academy, I will comply with the conditions set out in the Trust's ICT Acceptable Use Policy and will not:<br>● Use them for a non-educational purpose<br>● Use them without a teacher being present, or without a teacher's permission<br>● Use them to break academy rules<br>● Access any inappropriate websites or engage in inappropriate activity online<br>● Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)<br>● Use chat rooms<br>● Open any attachments in emails, or follow any links in emails, without first checking with a teacher<br>● Use any inappropriate language/images when communicating online, including in emails<br>● Share my password with others or log in to the academy's network using someone else's details<br>● Bully/harass other people<br>● Cause intentional damage to ICT facilities, network, software or data<br>● Use websites or mechanisms to bypass the academy's filtering or monitoring mechanisms<br>I understand that the academy will monitor the websites I visit and my use of the academy's ICT facilities and systems.<br>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.<br>I will comply with the academy's code of conduct for the use of AI.<br>I will always use the academy's ICT systems and internet responsibly.<br>I understand that the academy can discipline me if I do certain unacceptable things online, even if I'm not in the academy when I do them.</td></tr>
<tr><td>Signed (student):</td><td>Date:</td></tr>
<tr><td colspan="2">Parent/carer agreement: I agree to the conditions set out above for students using the academy's ICT systems and internet, and for using personal electronic devices in academy, and will make sure my child understands these.</td></tr>
<tr><td>Signed (parent/carer):</td><td>Date:</td></tr>
</table>

## Appendix 3: Acceptable use agreement for younger students

| **Acceptable use of the academy's ICT facilities and internet: agreement for students and parents/carers** | |
|---|---|
| **Name of student:** | |
| **When I use the academy's ICT facilities (like computers and equipment) and get on the internet in academy, I will not:**<br>● Use them without asking a teacher first, or without a teacher in the room with me<br>● Use them to break academy rules<br>● Go on any inappropriate websites<br>● Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson)<br>● Use chat rooms<br>● Open any attachments in emails, or click any links in emails, without checking with a teacher first<br>● Use mean or rude language or pictures when talking to other people online or in emails<br>● Share my password with others or log in using someone else's name or password<br>● Bully other people<br>● Damage the academy's equipment<br><br>I understand that the academy will check the websites I visit and how I use the academy's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.<br>I will tell a teacher or a member of staff I know immediately if I find anything on an academy computer or online that upsets me, or that I know is mean or wrong.<br>I will always be responsible when I use the academy's ICT systems and internet.<br>I understand that the academy can discipline me if I do certain unacceptable things online, even if I'm not in the academy when I do them. | |
| **Signed (student):** | **Date:** |
| **Parent/carer agreement:** I agree that my child can use the academy's ICT systems and internet when appropriately supervised by a member of academy staff. I agree to the conditions set out above for students using the academy's ICT systems and internet, and for using personal electronic devices in academy, 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 academy's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors** | |
|---|---|
| **Name of staff member/governor/volunteer/visitor:** | |
| When using the academy's ICT facilities and accessing the internet in academy, or outside academy on a work device, I will not:<br>● Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal, pornographic, racist or extremist nature (or create, share, link to or send such material)<br>● Access chat rooms or gambling sites<br>● Use any improper language/images when communicating online, including in emails or other messaging services<br>● Use them to bully or harass someone else, or to promote unlawful discrimination<br>● Use them in any way which could harm the academy's/trust's reputation<br>● Install any unauthorised software, or connect unauthorised hardware or devices to the academy's network<br>● Share my password with others or log in to the academy's network using someone else's details<br>● Share confidential information about the academy, its students or staff, or other members of the community<br>● Access, modify or share data I'm not authorised to access, modify or share<br>● Promote private businesses, unless that business is directly related to the academy<br>● Use websites or mechanisms to bypass the academy's filtering or monitoring mechanisms<br>● Using the academy's ICT facilities to breach intellectual property rights or copyright | |
| I understand that the academy will monitor the websites I visit and my use of the academy's ICT facilities and systems.<br>I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside the academy, and keep all data securely stored in accordance with this policy and the academy's data protection policy.<br>I will let the designated safeguarding lead (DSL) and ICT manager know if a student 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.<br>I will always use the academy's ICT systems and internet responsibly, and ensure that students 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 academy will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

| TERM | DEFINITION |
|---|---|
| **Antivirus** | Software designed to detect, stop and remove malicious software and viruses. |
| **Breach** | When your data, systems or networks are accessed or changed in a non-authorised way. |
| **Cloud** | Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices. |
| **Cyber attack** | An attempt to access, damage or disrupt your computer systems, networks or devices maliciously. |
| **Cyber incident** | Where the security of your system or service has been breached. |
| **Cyber security** | The protection of your devices, services and networks (and the information they contain) from theft or damage. |
| **Download attack** | Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent. |
| **Firewall** | Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network. |
| **Hacker** | Someone with some computer skills who uses them to break into computers, systems and networks. |
| **Malware** | Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations. |
| **Patching** | Updating firmware or software to improve security and/or enhance functionality. |

| TERM | DEFINITION |
|---|---|
| **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. |