ICT and Internet Acceptable Use Policy

Policy Reference	IT003
Author	Information Technology Director
Policy Agreed (date):	August 2025
Next Review (date):	January 2027
Approved by:	Managing Director

Contents

Version Control

Version	Author	Date	Changes
V 1.0	Managing Director	April 2024	Reviewed
V 1.1	HR Director	August 2024	Updated to reformat and include version control and reference number.
V 1.2	IT Manager	August 2025	Reviewed - Inserted statement about Friendly WiFi certification. Statement confirming unacceptable use around software, applications and digital services added.
V1.3	Information Technology Director	September 2025	Updated title of the IT Manager to Information Technology Director.
V 1.4	Information Technology Director	December 2025	Added reference to Social Media Policy.
V 1.5	HR Director	January 2026	References to Deputy Headteacher and Executive Headteacher to be read as Managing Director and Executive Leadership Team is Central Leadership Team. All policies to be updated by July 2026.

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our provision works, and is a critical resource for learners , staff (including the senior leadership team), volunteers and visitors.

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

This policy aims to:

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

This policy covers all users of our provision's ICT facilities, including executive leadership team, staff, learners, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our staff behaviour policy, disciplinary procedure or staff code of conduct.

2. 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 2025
- Searching, screening and confiscation: advice for provisions 2022
- National Cyber Security Centre (NCSC): Cyber Security for provisions
- 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 provisions and colleges

3. 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 provision's ICT service
Users	anyone authorised by the provision to use the provision's ICT facilities, including executive leadership team, staff, learners , volunteers, contractors and visitors
Personal use	any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user
Authorised personnel	employees authorised by the provision to perform systems administration and/or monitoring of the ICT facilities
Materials	files and data created using the provision's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix VI for a glossary of cyber security terminology.

4. Unacceptable use

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

Unacceptable use of the provision's ICT facilities includes:

- Using the provision's ICT facilities to breach intellectual property rights or copyright
- Using the provision's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the provision's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the provision, or risks bringing the provision into disrepute
- Sharing confidential information about the provision, its learners , or other members of the provision community
- Connecting any device to the provision's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the provision's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the provision's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the provision's ICT facilities

- Causing intentional damage to the provision's ICT facilities
- Removing, deleting or disposing of the provision's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the provision
- Using websites or mechanisms to bypass the provision's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- Using AI tools and generative chatbots (such as ChatGPT and Google Bard):
- During assessments, including internal and external assessments, and coursework
- Downloading, installing, or attempting to install any programs, software, applications, or browser extensions on any organisation-owned devices without prior written authorisation from the Information Technology Director.
- Signing up to, registering for, or creating accounts with any online or digital service, platform, or subscription on behalf of the organisation without prior authorisation from the Information Technology Director.

This is not an exhaustive list. The provision reserves the right to amend this list at any time. The Executive Leadership Team will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the provision's ICT facilities.

Exceptions from unacceptable use

Where the use of provision ICT facilities (on the provision 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 Managing Director's discretion. This must be put in writing to the Managing Director.

Sanctions

Learners and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the provision's policies on staff behaviour policy, disciplinary policy or staff code of conduct.

5. Staff

Access to provision ICT facilities and materials

The provision's Information Technology Director manages access to the provision's ICT facilities and materials for provision staff. That includes, but is not limited to:

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

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

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Information Technology Director.

Only approved software and digital services that have been evaluated for compatibility, licensing, safeguarding, and data protection requirements may be installed or used. Any unauthorised installation, registration, or subscription may result in removal of access rights and could lead to disciplinary action. Requests for additional software or access to digital services should be submitted to the Information Technology Director, who will review the need, security risks, licensing, safeguarding, and data protection implications before granting approval.

Use of phones and email

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

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

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

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

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

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

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

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

If staff send an email in error that contains the personal information of another person, they must inform the Data Protection Officer (Marcus Griggs) immediately and follow the provisions personal data breach procedure.

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

Work phones must not be used for personal matters.

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

Using personal devices for work purposes

To protect the security of data and maintain compliance with safeguarding and data protection requirements:

- Staff must **not access work-related information, accounts, or systems** (including but not limited to Google Drive, Gmail, MIS platforms, safeguarding systems, or any other provision-related accounts) on personal devices.
- Work information must only be accessed using **provision-issued devices** that are configured with appropriate security settings and monitoring.
- This restriction applies to **all forms of access**, including web browsers, apps, and email clients on personal devices.

- Any breach of this requirement may be treated as a **disciplinary matter** under the provision's staff code of conduct.

Personal use

Staff are permitted to use provision ICT facilities for personal use with permission from the Managing Director, subject to certain conditions set out below. This permission must not be overused or abused. The Information Technology Director may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not take place during provision hours
- Does not constitute 'unacceptable use', as defined in Unacceptable use
- Does not interfere with their jobs, or prevent other staff or learners from using the facilities for work or educational purposes

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

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

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

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

Personal social media accounts

Members of staff are expected to maintain appropriate professional boundaries and conduct when using social media, whether for work-related or personal purposes, and regardless of privacy settings, platform, device, or time of use.

Staff must ensure that their personal use of social media does not compromise safeguarding, confidentiality, data protection, or the reputation of the provision. Privacy settings may reduce risk but do not remove professional accountability.

Staff are required to follow the provision's **Social Media Policy**, including guidance on appropriate privacy and security settings, professional boundaries, and reporting concerns. Any safeguarding, data protection, or conduct issues arising from social media use must be reported immediately in line with provision procedures.

The provision has guidelines for staff on appropriate security settings for social media accounts (see Social Media policy, appendix II).

Remote access

We allow staff to access the provision's ICT facilities and materials remotely, only from a company-issued device.

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

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

Provision social media accounts

The provision maintains official social media accounts, which are managed solely by authorised members of the Senior Leadership Team and the Executive Lead for Data, Security and Compliance. Staff who have not been formally authorised to manage or post to these accounts must not access, attempt to access, or engage with them in any way.

All content posted on official provision social media accounts must comply with the **Social Media Policy**, including guidelines on safeguarding, data protection, consent, and age-appropriate communication. Authorised staff are responsible for ensuring that all posts, comments, and interactions adhere to these guidelines at all times.

Unauthorised access or breaches of these guidelines may result in disciplinary action in line with the Staff Code of Conduct.

Monitoring and filtering of the provision network and use of ICT facilities

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

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

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

The provision monitors ICT use in order to:

- Obtain information related to provision business
- Investigate compliance with provision policies, procedures and standards
- Ensure effective provision 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

The Information Technology Director and designated leads will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the provision's DSL and Information Technology Director, as appropriate.

6. Learners

Access to ICT facilities

ICT facilities available to learners are as follows:

- Computers and equipment in the provision's computer suite are available to learners only under the supervision of staff
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff
- Tablets & smart boards are available to learners under 1:1 supervision of staff.

Search and deletion

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

- Poses a risk to staff or learners , and/or
- Is evidence in relation to an offence

This includes, but is not limited to:

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

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

- Make an assessment of how urgent the search is, and consider the risk to other learners and staff. If the search is not urgent, they will seek advice from the Information Technology Director.
- Explain to the learner 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 learner's co-operation

The authorised staff member should:

- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a learner was in possession of a banned item.
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

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

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

- Cause harm, and/or
- Undermine the safe environment of the provision or disrupt teaching, and/or

- Commit an offence

If inappropriate material is found on the device, it is up to the DSL and Managing Director to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

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

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

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

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

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

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

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

Unacceptable use of ICT and the internet outside of provision

The provision will sanction learners, in line with the behaviour policy if a learner engages in any of the following at any time (even if they are not on provision 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 provision's policies or procedures
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the provision, or risks bringing the provision into disrepute
- Sharing confidential information about the provision, other learners , or other members of the provision 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 provision's ICT facilities
- Causing intentional damage to the provision's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

7. Parents/ Carers

Access to ICT facilities and materials

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

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

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

Communicating with or about the provision online

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

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

We ask parents/carers to sign the agreement in appendix II and appendix III.

Communicating with parents/carers about learner activity

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

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

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

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

8. Data security

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

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

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

Passwords

All users of the provision's ICT facilities should set strong passwords for their accounts and keep these passwords secure, whilst enabling multi-factor authentication (MFA).

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

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

Software updates, firewalls and anti-virus software

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

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

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

Data protection

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

Access to facilities and materials

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

These access rights are managed by the Information Technology Director.

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 Information Technology Director immediately.

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

Encryption

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

9. Protection from cyber attacks

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

The provision will:

- Work with Executive Leadership Team and the IT department to make sure cyber security is given the time and resources it needs to make the provision secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the provision's annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details
    - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Ensure staff are aware that the provision does not permit personal devices to be connected to the provisions' network.
- 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 provision will verify this using a third-party audit (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 provision 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 the drive.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to the Managing Director.
- Make sure staff:
    - Enable multi-factor authentication where they can, on things like provision email accounts
    - Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the provision 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 provision 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'

10. Internet access

The Provision's wireless internet connection is secure.

Access to the Provision's WiFi is available freely to members of staff, and with authorisation from the Managing Director to visitors. All users will be made aware of standard filtering installed by the network provider, with the addition of locally installed filtering & monitoring software, Senso.cloud.

Should access to specific websites be available/not available when it is believed that the filtering is incorrect, they should inform the Data Manager at their earliest convenience.

The provision's wireless internet connection is certificated by Friendly WiFi, further confirming that the WiFi is filtered for inappropriate content.

Parents/carers and visitors

Parents/carers and visitors to the provision will not be permitted to use the provision's WiFi unless specific authorisation is granted by the Managing Director.

The Managing Director will only grant authorisation if:

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

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

11. Monitoring arrangements

The Managing Director and Information Technology Director will monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the provision.
This policy will be reviewed annually.

12. Links with other policies

This policy should be read alongside the policies on::

- Online Safety Policy
- Safeguarding and Child Protection Policy
- Behaviour Policy
- Disciplinary Procedure
- Data Protection Policy
- Social Media Policy

Appendix I - Facebook cheat sheet for staff

Do not accept friend requests from learners on social media

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

Check your privacy settings

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

- In the first instance, ignore and delete the request. Block the learner from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture

- If the learner asks you about the friend request in person, tell them that you're not allowed to accept friend requests from learners and that if they persist, you'll have to notify senior leadership and/or their parents/carers. If the learner persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the Managing Director 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 provision
- learners 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 learner 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 II - KS1 acceptable use agreement (learners and parents/carers)

ACCEPTABLE USE OF THE PROVISION'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR LEARNERS AND PARENTS/CARERS	
Name of learner:	
When I use the provision's ICT systems (like computers) and get onto the internet in provision I will: ● Ask a teacher or adult if I can do so before using them ● Only use websites that a teacher or adult has told me or allowed me to use ● Tell my teacher immediately if: ○ I click on a website by mistake ○ I receive messages from people I don't know ○ I find anything that may upset or harm me or my friends ● Use provision computers for provision work only ● Be kind to others and not upset or be rude to them ● Look after the provision ICT equipment and tell a teacher straight away if something is broken or not working properly ● Only use the username and password I have been given ● Try my hardest to remember my username and password ● Never share my password with anyone, including my friends ● Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer ● Save my work on the provision network ● Check with my teacher before I print anything ● Log off or shut down a computer when I have finished using it	
I agree that the provision will monitor the websites I visit and that there will be consequences if I don't follow the rules.	
Signed (learner):	
Date:	
Parent/carer agreement:	
I agree that my child can use the provision's ICT systems and internet when appropriately supervised by a member of provision staff. I agree to the conditions set out above for learners using the provision's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	
Date:	

Appendix III - KS2, KS3 & KS4 acceptable use agreement (learners and parents/carers)

ACCEPTABLE USE OF THE PROVISION'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR LEARNERS AND PARENTS/CARERS	
Name of learner:	

I will read and follow the rules in the acceptable use agreement policy. When I use the provision's ICT systems (like computers) and get onto the internet in provision I will:

- Always use the provision's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Log in to the provision's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into provision:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the provision, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the provision will monitor the websites I visit and that there will be consequences if I don't follow the rules.	
Signed (learner):	
Date:	
Parent/carer agreement:	
I agree that my child can use the provision's ICT systems and internet when appropriately supervised by a member of provision staff. I agree to the conditions set out above for learners using the provision's ICT systems and internet, and for using personal electronic devices in provision, and will make sure my child understands these.	
Signed (parent/carer):	
Date:	

Appendix IV - Acceptable use agreement (staff, volunteers & visitors)

ACCEPTABLE USE OF THE PROVISION'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, VISITORS & VISITORS	
Name of staff member/volunteer/visitor:	

When using the provision's ICT systems and accessing the internet in provision, or outside provision on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the provision's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the provision's network
- Share my password with others or log in to the provision's network using someone else's details
- Take photographs of learners without checking with teachers first
- Share confidential information about the provision, its learners or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the provision

I will only use the provision's ICT systems and access the internet in provision, or outside provision on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the provision will monitor the websites I visit and my use of the provision's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside provision, and keep all data securely stored in accordance with this policy and the provision's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a learner informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the provision's ICT systems and internet responsibly, and ensure that learners in my care do so too.

Signed (staff member/volunteer/visitor):	
Date:	

Appendix VI - Glossary of cyber security terminology

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

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

TERM	DEFINITION
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.