IT & E SAFETY POLICY

CONTENTS

FOREWORD

Freedom Foundation Portway Alternative Provision, Freedom Foundation Dunkirk Alternative Provision are all sites for KS1 & KS2 Alternative Provision. They are referred to as Freedom Foundation AP for the benefit of students and this document.

01 AIMS

Information and communications technology (ICT) is an integral part of the way we work, and is a critical resource for students, AP staff, volunteers, and visitors. It supports teaching and learning, and the pastoral and administrative functions of the alternative provision.

However, the ICT resources and facilities our alternative 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 ICT resources for staff, students, and parents/carers
- Establish clear expectations for the way all members of the AP community engage with each other online
- Support the AP's policies on data protection, online safety, and safeguarding
- Prevent disruption that could occur to the trust through the misuse, or attempted misuse, of ICT systems
- Support the teaching of safe and effective internet and ICT use

This policy covers all users of our AP's ICT facilities, including AP staff, students, volunteers, contractors, and visitors.

Any breach of this policy may result in disciplinary or behaviour proceedings.

02 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 2024

- Searching, screening and confiscation: advice for schools 2022

- National Cyber Security Centre (NCSC): Cyber Security for Schools

- Education and Training (Welfare of Children) Act 2021

- UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

- Meeting digital and technology standards in schools and colleges

03 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 AP's ICT service.

Users: Anyone authorised by the AP to use the ICT facilities, including staff, students, 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 AP to perform systems administration and/or monitoring of the ICT facilities.

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

See Appendix 5 for a glossary of cyber security terminology.

04 UNACCEPTABLE USE

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

Unacceptable use of the AP's ICT facilities includes:

- Using the ICT facilities to breach intellectual property rights or copyright

- Using the ICT facilities to bully or harass someone else, or to promote unlawful discrimination

- Breaching the AP'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 AP, or risks bringing the AP into disrepute

- Sharing confidential information about the AP, its students, or other members of the AP's community

- Connecting any device to the AP's ICT network without approval from authorised personnel

- Setting up any software, applications or web services on the AP'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 AP'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 AP's ICT facilities

- Causing intentional damage to the AP's ICT facilities

- Removing, deleting or disposing of the AP'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 AP

- Using websites or mechanisms to bypass the AP's filtering or monitoring mechanisms

- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

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

04.1 EXCEPTIONS FROM UNACCEPTABLE USE

Where the use of AP ICT facilities (on the AP 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 head of provision's discretion. The head of provision must be contacted first and confirmation of approval will be sent via email.

Staff may use AI and generative chatbots:

- As a research tool to help them find out about new topics and ideas
- To support internal larger projects eg bid writing

Freedom Foundation AP enforces a 'no phones' policy, creating an online technology-free environment. Students may have access to devices (an ipad), when necessary and fully supervised by the lead facilitator, but internet use will be limited to music software only.

04.2 SANCTIONS

Students and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the AP's policies on behaviour, disciplinary procedure, and staff code of conduct.

05 STAFF (INCLUDING VOLUNTEERS AND CONTRACTORS)

05.1 ACCESS TO AP ICT FACILITIES AND MATERIALS

The AP head of provision manages access to the AP's ICT facilities and materials for the AP 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 AP'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 AP head of provision.

05.2 USE OF PHONES AND EMAIL

Freedom Foundation AP 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.

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

Staff must not share their personal email addresses with parents/carers and students 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 head of provision immediately and follow our data breach procedure.

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

AP 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 section 4.

The AP can record incoming and outgoing phone conversations.

Staff who would like to record a phone conversation should speak to the head of provision.

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

Requests to record conversations may be granted for the following:

- Discussing a complaint raised by a parent/carer or member of the public
- Calling parents/carers to discuss behaviour or sanctions
- Taking advice from relevant professionals regarding safeguarding, special educational needs (SEN) assessments, etc.
- Discussing requests for term-time holidays

05.3 PERSONAL USE

Staff are permitted to occasionally use AP ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The head of provision 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 contact time or teaching hours
- 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 may not use the AP'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 AP's ICT facilities for personal use may put personal communications within the scope of the AP's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the AP's Safeguarding Policy.

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

Staff should take care to follow the AP's guidelines on use of social media (see appendix 1) and use of email (see section 5.2) to protect themselves online and avoid compromising their professional integrity.

05.4 PERSONAL SOCIAL MEDIA ACCOUNTS

Members of staff should make sure their use of social media, either for work or personal purposes, is always appropriate.

The AP has guidelines for staff on appropriate security settings for social media accounts (see appendix 1).

05.5 REMOTE ACCESS

We allow staff to access the AP's ICT facilities and materials remotely.

Staff accessing the AP'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 AP's ICT facilities outside the AP and must take such precautions as the head of provision 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.

05.6 AP SOCIAL MEDIA ACCOUNTS

Freedom Foundation has an official Facebook / X / Instagram account, managed by the senior leadership team. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

The AP has guidelines for what may and for what must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they always abide by these guidelines.

05.7 MONITORING AND FILTERING OF THE AP NETWORK AND USE OF ICT FACILITIES

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the AP 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
- Use activity/access logs
- Any other electronic communications

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

The AP monitors ICT use in order to:

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

Freedom Foundation's Directors are responsible for making sure that:

- The AP meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
    - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- They regularly review the effectiveness of the AP's monitoring and filtering systems

The AP's designated safeguarding lead (DSL) will take responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the AP's DSL and head of provision, as appropriate.

06 STUDENTS

06.1 ACCESS TO ICT FACILITIES

Computers and equipment in the AP will not be available to students.

Students may have access to devices (an ipad), when necessary and fully supervised by the lead facilitator, but internet use will be limited to music software only.

06.2 SEARCH AND DELETION

Freedom Foundation AP enforces a 'no phones' policy, creating an online technology-free environment.

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

- Poses a risk to staff or students, and/or
- Is identified in the AP rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography

- Abusive messages, images or videos

- Indecent images of children

- Evidence of suspected criminal behaviour (such as threats of violence or assault)

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

- Access how urgent the search is and consider the risk to other students and staff. If the search is not urgent, they will seek advice from the designated safeguarding lead and home school

- Explain to the student 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 student's co-operation

The authorised staff member should:

- Inform the DSL and Home School of any searching incidents where they had reasonable grounds to suspect a student was in possession of a banned item such as drugs, alcohol, weapons, illegal vapes and other dangerous items.

- Involve the DSL without delay if they believe that a search has revealed a safeguarding risk. The DSL must then communicate the risk to the Home School

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 AP or disrupt teaching, and/or

- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL and Home

School 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 student and/or the parent refused 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 immediately, who will communicate the concern with the Home School and decide what to do next. The Home School will make the decision in line with the DfE's latest guidance on searching, screening and confiscating 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 students will be carried out in line with:

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

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

06.3 UNACCEPTABLE USE OF ICT AND THE INTERNET OUTSIDE OF THE AP

The AP will sanction students, in line with the behaviour policy, if a student engages in any of the following at any time (even if they are not on the 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 AP'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 AP, or risks bringing the AP into disrepute

- Sharing confidential information about the AP, other students, or other members of the AP 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 AP's ICT facilities

- Causing intentional damage to the AP'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

07 PARENTS/CARERS

07.1 ACCESS TO ICT FACILITIES AND MATERIALS

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

07.2 COMMUNICATING WITH OR ABOUT THE AP ONLINE

We believe it is important to model for students, 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 AP through our website and social media channels.

We ask parents/carers to sign the agreement in Appendix 2.

07.3 COMMUNICATING WITH PARENTS/CARERS ABOUT STUDENT ACTIVITY

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

When we ask students 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 are shared.

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

08 DATA SECURITY

The AP is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and students. 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, students, parents/carers and others who use the AP's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education’s guidance on digital and technology standards in schools and colleges, including the use of:

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

08.1 PASSWORDS

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

Passwords must be at least 10 characters long containing letters and numbers. Staff are reminded that they should not reuse passwords from other sites.

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

Members of staff who disclose account or password information may face disciplinary action.

08.2 SOFTWARE UPDATES, FIREWALLS, AND ANTI-VIRUS SOFTWARE

All of the AP’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 AP’s ICT facilities.

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

08.3 DATA PROTECTION

All personal data must be processed and stored in line with data protection regulations and the AP’s data protection policy (which can be found on the website).

08.4 ACCESS TO FACILITIES AND MATERIALS

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

These access rights are managed by the head of provision.

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 head of provision 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.

08.5 ENCRYPTION

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

AP staff may only use personal devices (including computers and USB drives) to access AP data, work remotely, or take personal data (such as student information) out of the premises if they have been specifically authorised to do so by the head of provision.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption.

09 PROTECTION FROM CYBER ATTACKS

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

The AP will:

- Work with Freedom Foundations Directors and the IT department to make sure cyber security is given the time and resources it needs to make the AP secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the AP's annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information, or login details
    - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
    - Proportionate: the AP will verify this using a third-party audit at least annually, 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 AP needs to update its software
    - Regularly reviewed and tested: to make sure they systems are as effective and secure as they can be
- Back up critical data at least once a day and store these backups on cloud-based backup systems
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our cloud-based provider

- Make sure staff:
    - Dial into our network using a virtual private network (VPN) when working from home
    - Enable multi-factor authentication where they can, on things like AP email accounts
    - Store passwords securely using a password manager
- Make sure the Head of Provision conducts regular access reviews to make sure each user in the AP 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 AP 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 every 6 months and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

10 INTERNET ACCESS

The AP's wireless internet connection is secured, filtered and monitored, with separate connections for staff, students and visitors.

In line with the AP's safeguarding and prevent responsibilities, the use of the AP network is carefully monitored and recorded. Freedom Foundation AP use web filtering software to secure, monitor and limit certain websites.

10.1 STUDENTS

Wi-Fi and the AP's network/IT facilities are provided for educational, research, and personal development use of all members of the AP's community.

Students must use the AP's Wi-Fi service for internet access (if required) during the day.

10.2 PARENTS/CARERS AND VISITORS

Parents/carers and visitors to the AP will not be permitted to use the AP's Wi-Fi unless specific authorisation is granted by the head of provision.

The head of provision will only grant authorisation if:

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

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

11 RELATED POLICIES

This policy should be read alongside the AP’s policies on:

- Social Media
- Safeguarding and Child Protection
- Behaviour
- Staff Discipline
- Data Protection
- Remote Education

12 REVIEW

We keep this policy under regular review:

Review of this Policy: April 2025
Next Review Date: April 2026
Reviewed By: Laura Grant
Position/Role: Director of Freedom Foundation

APPENDIX 1: SOCIAL MEDIA CHEAT SHEET FOR STAFF

DO NOT ACCEPT FRIEND REQUESTS FROM STUDENTS ON SOCIAL MEDIA

10 rules for staff on social media

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 AP hours

7. Don't make comments about your job, your colleagues, our AP or your students online – once it's out there, it's out there

8. Don't associate yourself with the AP on your profile (e.g., by setting it as your workplace, or by 'checking in' at an 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 social media apps from your phone. The app recognises Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi 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 on Facebook

- 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 on Facebook

- 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...

1. 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 head of provision about what's happening

2. A parent/carer adds you on social media:

   - It is at your discretion whether to respond. Bear in mind that:

     - Responding to one parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the AP

     - 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

3. You are 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 OF THE INTERNET: AGREEMENT FOR PARENTS /CARERS

ACCEPTABLE USE OF THE INTERNET: AGREEMENT FOR PARENTS/CARERS

Name of Parent/Carer:	**Name of Child:**

Online channels are an important way for parents/carers to communicate with, or about, our AP.

The school uses the following channels:

- Our official Facebook, X, and Instagram page
- Email/text groups for parents/carers (for AP announcements and information)
- Our virtual learning platform

Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).

When communicating with the AP via official communication channels, or using private/independent channels to talk about the AP:

I will:

- Be respectful towards members of staff, and the AP, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the AP's official channels, so they can be dealt with in line with the AP's complaints procedure

I will not:

- Use private groups, the AP's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive, and the AP can't improve or address issues unless they are raised in an appropriate way
- Use private groups, the AP's Facebook page, or personal social media to complain about, or try

<table>
<tr><td colspan="2">to resolve, a behaviour issue involving other students. I will contact the AP and speak to the appropriate member of staff if I’m aware of a specific behaviour issue or incident
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other children’s parents/carers</td></tr>
<tr><td><b>Signed:</b></td><td><b>Date:</b></td></tr>
</table>

APPENDIX 3: ACCEPTABLE USE AGREEMENT FOR YOUNGER STUDENTS

ACCEPTABLE USE OF THE AP'S ICT FACILITIES AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS

Name of Student:

When I use the AP’s ICT facilities (like computers and equipment) and go on the internet on the premises:

I will not:

- Use them without asking a teacher first, or without a teacher in the room with me
- Use them to break AP rules
- Go on any inappropriate websites
- Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson)
- Use chat rooms
- Open any attachments in emails, or click any links in emails, without checking with a teacher first
- Use mean or rude language when talking to other people online or in emails
- Send any photos, videos or livestreams of people (including me) who aren’t wearing all of their clothes
- Share my password with others or log in using someone else’s name or password
- Bully other people
- Use artificial intelligence (AI) chatbots, such as ChatGPT or Google Bard, to create images or write for me, and then submit it as my own work

I understand that the AP will check the websites I visit and how I use the AP’s computers and equipment. This is so that they can help keep me safe and make sure I’m following the rules.

I will tell a teacher or a member of staff I know immediately if I find anything on an AP computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use the AP's ICT systems and internet.

I understand that the AP can discipline me if I do certain unacceptable things online, even if I’m not in the AP when I do them.

Signed (Student):	**Date:**

Parent/carer agreement:
I agree that my child can use the AP’s ICT systems and internet when appropriately supervised by a member of AP staff. I agree to the conditions set out above for students using the AP’s ICT systems and internet, and for using personal electronic devices in the AP, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

APPENDIX 4: ACCEPTABLE USE AGREEMENT FOR AP STAFF, VOLUNTEERS, AND VISITORS

ACCEPTABLE USE OF THE AP'S ICT FACILITIES AND INTERNET: AGREEMENT FOR AP STAFF, VOLUNTEERS, AND VISITORS

Name of AP Staff Member/Volunteer/Visitor:

When I use the AP’s ICT facilities and accessing the internet in the AP, or outside of the premises on a work device:

I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the AP’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 AP's network
- Share my password with others or log in to the AP's network using someone else’s details
- Share confidential information about the AP, its students or staff, or other members of the community
- Access, modify or share data I’m not authorised to access, modify or share
- Promote any private business, unless that business is directly related to the AP

I understand that the AP will monitor the websites I visit and my use of the AP’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 the AP, and keep all data securely stored in accordance with this policy and the AP's data protection policy.

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.

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

Signed (AP staff member/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 AP will put in place. They are 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	When your data, systems or networks are accessed or changed in a non-authorised way.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate

	website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infected 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.