Ox Close Federation

Acceptable Use Policy

Approved	**October 2023**
Review Date	**October 2024**

1. Introduction and Aims

The purpose of the policy is to ensure the Federation network is operated safely and all users of ICT are safe. It refers to our ICT network and to the use of mobile technologies, both within it and external to it, explains the behaviours which are acceptable and unacceptable within Ox Close Federation.

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

However, the ICT resources and facilities used also pose risks to data protection, online safety and safeguarding.

This policy aims to:

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

This policy covers all users of our Federation's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

All members of staff have a responsibility to use the Federation's computer system in a professional, lawful, and ethical manner. Our AUP must be fully complied with at all times. All users of the Federation network should note that it is monitored on a regular basis. Any person who is found to have misused the Federation system or not followed our AUP could face disciplinary action and in the most serious cases legal action may also be taken.

2. Legislation and Guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- 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
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2021
- Searching, screening and confiscation: advice for schools
- National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021

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, communication applications such as WhatsApp, Facebook messenger, SMS messaging 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 Federation to use the ICT facilities, including governors, staff, pupils, 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 Federation 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

4. Unacceptable Use

The following is considered unacceptable use of the Federation's ICT facilities and online platforms by any member of the Federation community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the Federation's ICT facilities includes:

- Using the Federation's ICT facilities to breach intellectual property rights or copyright.
- Using the Federation's ICT facilities to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the Federation's policies or procedures.
- Any illegal conduct, or 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.
- Activity which defames or disparages the Federation, or risks bringing the Federation into disrepute.
- Sharing confidential information about the Federation, its pupils, or other members of the Federation community.
- Connecting any device to the Federation's ICT network without approval from authorised personnel.
- Setting up any software, applications or web services on the Federation'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 Federation'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.
- Using inappropriate or offensive language.
- Promoting a private business, unless that business is directly related to the Federation.
- Using websites or mechanisms to bypass the Federation's filtering mechanisms.

This is not an exhaustive list. The Federation reserves the right to amend this list at any time. The Executive Headteacher or other delegated member of FLT will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the Federation's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of Federation ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion.

In such circumstances, permission must be sought from the Executive Headteacher.

4.2 Sanctions

Staff or pupils who engage in any of the unacceptable activity listed above may face disciplinary action in line with the Federation's policies including the Behaviour Policy (Pupils), Disciplinary Policy and Staff Code of Conduct (Staff).

In the case of adults who are not staff members other sanctions are available such as revoking permission to use the Federation's systems.

Members of staff will have been provided access to the above policies as part of your induction. If you require access to a copy these are available from the Executive Headteacher or office.

5. Staff (including governors, volunteers, supply teachers and contractors)

5.1 Access to Federation ICT facilities and materials

The Executive Headteacher manages access to the Federation's ICT facilities and materials for Federation staff. That includes, but is not limited to:

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

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the Federation's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the headteacher or ICT Technician.

5.1.1 Use of phones and email

The Federation 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 Federation has provided.

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

E-mail attachments should only be opened if the source is known and trusted. There have been an increasing number of spam emails received by staff in schools which contain links that can be damaging to ICT systems and also lead to serious network and equipment hacking.

If you are required to send an email to more than one recipient, ensure that the email addresses are entered in to the 'bcc' box to ensure that you are not sharing personal email addresses with others.

E-mail should be written carefully and politely and should never contain anything which is likely to cause annoyance, inconvenience or needless anxiety. 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 and public.

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. A double-checking system should also be implemented whereby one member of staff asks another to check content of their message before sending

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 which contains the personal information of another person, they must inform the headteacher or data protection officer immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the Federation to conduct all work-related business.

Federation 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.

If for any reason a member of staff feels there is a need to attempt to record a telephone conversation this should be discussed first with the Executive Headteacher.

5.1.2 Use of printers

If printing or scanning documents, ensure that any document containing personal or sensitive information is only printed at a time when you are able to collect it immediately, so as not to leave sensitive information lying on printers/photocopiers

5.2 Personal use

Staff are permitted to occasionally use Federation ICT facilities and mobile phones for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The headteacher may withdraw permission for it at any time or restrict access at their discretion.

ICT facilities personal use is permitted provided that such use:

- Does not take place during worktime.
- Does not constitute 'unacceptable use', as defined in section 4.
- Takes place when no pupils are present.
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes.

Staff may not use the Federation'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 Federation's ICT facilities for personal use may put personal communications within the scope of the Federation's ICT monitoring activities (see section 5.5). 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 Federation ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

Personal mobile phones should not be used in areas of Federation where pupils have access

During teaching time, mobile phones should be turned off or put on silent mode and stored in an area away from sight of the children.

Staff are allowed to access their personal phones on breaks, lunch times and after Federation in designated areas e.g. staff room (safe, suitable places where the children are not present).

It is forbidden to take photographs/videos of the children on personal mobile phones.

Staff should take care to follow the Federation's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times. Remember that damage to professional reputations can inadvertently be caused by quite innocent postings or images.

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

5.2.2 Communication platforms

Members of staff should consider how they communicate with each other both inside and outside of Federation when discussing any work matters. This includes during personal time on messaging platforms such as Whatsapp and Messenger. Remember that what you may deem as 'personal' messages could unintentionally become public and therefore if Federation matters are being discussed you should consider carefully your use of language and subject matter.

Ox Close Federation will always encourage staff that any messages relating to Federation, even in 'personal' forums should be written carefully and politely and should never contain anything which is likely to cause annoyance, inconvenience or needless anxiety. Incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

5.3 Remote Access

We allow staff to access the Federation's ICT facilities and materials remotely through Office 365 and our cloud platform.

Staff accessing the Federation'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 Federation's ICT facilities outside the Federation and take such precautions as the Federation may require from time to time 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.

No Federation related information should be stored on any personal equipment. You must not download or save any information onto personal equipment such as mobile phones or laptops/PCs.
If you have a need to work offsite and require electronic or paper-based information to be taken from Federation to work on you must

- First seek permission from the head teacher for the removal of the information e.g. pupil file, laptop, encrypted Federation memory stick
- Ensure the secure transit of the information
- Ensure that no information is downloaded or stored on personal equipment
- Be aware of other people within the immediate area when viewing personal or sensitive information in areas outside of Federation and limiting such activity away from public places

5.4 Federation social media accounts

Any social media accounts operated by the Federation will be managed by a named person or persons. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The Federation has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

5.5 Images of pupils

All pupils need parental permission to have photographs or videos published electronically or in a public area even if they are unidentifiable. If in doubt as to whether a pupil has permission you must check with the Federation office before publishing/displaying.

No photos or videos which include nudity or inappropriate actions are permitted to be taken or downloaded under any circumstance.

Images of students must be stored in the designated area of the ICT network/Cloud. It is not permitted to remove images off site (on camera, phone or storage device).

Images should be deleted from electronic devices once after uploading to the above storage area

5.6 Monitoring of Federation network and use of ICT facilities

The Federation reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

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

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

The Federation monitors ICT use in order to:

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

6. Pupils

6.1 Access to ICT facilities

- Activities should be planned by staff so that 'open searching is kept to a minimum.
- Computers and equipment in Federation are available to pupils only under the supervision of staff
- When searching the internet with pupils, adults should encourage the children to use 'child safe' search engines if applicable (depending on age)

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the Federation has the right to search pupils' phones, computers or other devices for any data or items banned under Federation rules or legislation.

The Federation 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 Federation's rules.

6.3 Unacceptable use of ICT and the internet outside of Federation

The Federation will sanction pupils, in line with the behaviour policy, if a pupil engages in any of the following **at any time** (even if they are not on Federation 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 Federation's policies or procedures.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Accessing, creating, storing, linking to or sending material that is offensive, obscene or otherwise inappropriate.
- Activity which defames or disparages the Federation, or risks bringing the Federation into disrepute.
- Sharing confidential information about the Federation, other pupils, or other members of the Federation 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 Federation's ICT facilities.
- Causing intentional damage to ICT facilities or materials.
- 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.
- Using inappropriate or offensive language.

7. Parents

7.1 Access to ICT facilities and materials

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

However, parents working for, or with, the Federation in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the Federation's facilities at the headteacher's discretion.

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

7.2 Communicating with or about the Federation online

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

We ask parents to sign the agreement in appendix 2.

8. Data Security

The Federation takes steps to protect the security of its computing resources, data and user accounts. However, the Federation cannot guarantee security. Staff, pupils, parents and others who use the Federation's ICT facilities should use safe computing practices at all times.

8.1 Passwords

Each adult working within the Federation must log on to the computers using the username and password given to them (class account or individual account) and these must be changed to an individual specific password where stated. Passwords need to be kept a secret, not written down and stored in or around the computer. If for any reason an adult needs to leave their computer, they have to lock the computer to prevent others from using their account by pressing 'Ctrl, Alt and Delete'.

Any supply teachers or visitors to the Federation must see our Executive Headteacher to obtain a guest account and password. Their password will need to be kept private and not shared.

You should ensure you use dual factor authentication when possible if dealing with sensitive information- for example CPOMS.

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 pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

8.2 Software updates, firewalls, and anti-virus software

All of the Federation's ICT devices that support software updates, security updates, and anti-virus products will 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 Federation's ICT facilities.

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

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the Federation's data protection policy. Data protection policy requires that any staff or student / pupil data to which members of staff have access, will be kept private and confidential, except when it is deemed necessary that by a requirement of law or by Federation policy to disclose such information to an appropriate authority.

8.4 Access to facilities and materials

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

These access rights are managed by the headteacher.

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 headteacher immediately.

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

8.5 Encryption

The Federation ensures that its devices and systems have an appropriate level of encryption. Therefore, personal equipment such as USB sticks or other personal devices are not permitted.

9. Protection from Cyber Attacks

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

The Federation will:

- Work with governors and our ICT technician service to make sure cyber security is given the time and resources it needs to make the Federation secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the Federation'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 Federation will verify this using a third-party audit at least annually to objectively test that what it has in place is up to scratch
    - **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 Federation needs to update its software
    - **Regularly reviewed and tested**: to make sure the systems are as up to scratch and secure as they can be
- Back up critical data regularly and store these backups on [cloud based backup systems/external hard drives that aren't connected to the Federation network and which can be stored off the Federation premises]
- Delegate specific responsibility for maintaining the security of our management information system (MIS)
- 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 Federation email accounts
    - Store passwords securely using a password manager
- Make sure we conduct regular access reviews to make sure each user in the Federation has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Develop, review and test an incident response plan with the IT department, for example, including how the Federation will communicate with everyone if communications go down, who will be contacted when, and who will notify Action Fraud of the incident. This will be reviewed and tested at least annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
- Work with our Local Authority to see what it can offer the Federation regarding cyber security, such as advice on which service providers to use or assistance with procurement

10. Internet Access

The Federation wireless internet connection is secured and content filtering is in operation. If you should happen to access an inappropriate site that the filter has not identified, or 'safe' sites that are filtered in error, please inform the headteacher or ICT Technician.

10.1 Parents and visitors

Parents and visitors to the Federation will not be permitted to use the Federation's WIFI unless specific authorisation is granted by the Executive Headteacher

The Executive Headteacher will only grant authorisation if:

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

The Executive Headteacher monitors the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the Federation.

This policy will be reviewed every year.

The Policy Alignment and Approval committee are responsible agreeing this policy.

12. Related policies

This policy should be read alongside the Federation's policies on:

- Online Safety
- Safeguarding and Child Protection
- Behaviour Policy
- Disciplinary Policy
- Data Protection Policy
- Use of Photographic Images Policy
- Staff Code of Conduct

Appendix 1: Facebook guidance sheet for staff

Don't accept friend requests from pupils on social media

12 rules for school staff on Facebook

1. Consider changing 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 not, ensure 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 just as happy showing your pupils
6. Don't use personal social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)
11. Consider very carefully any friend requests from parents/carers
12. Never use facebook to respond to parents/carers regarding queries or questions around school business

---

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What do to if…

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the Federation
    - Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
    - Parent's sometimes feel that they can contact you through your personal Facebook account to ask questions or raise issues in relation to the Federation. To respond to such communication would be in breach of Federation policies
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent 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 and carers

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our Federation. The Federation uses the following channels: • Our official Facebook pages. • Email/text groups for parents (for school announcements and information). • Microsoft Teams • SeeSaw Parents/carers also sometimes 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). Please note that Federation has no responsibility for the running or content for such groups.	
When communicating with the Federation via official communication channels, or using private/independent channels to talk about the Federation, I will: • Be respectful towards members of staff, and the Federation, at all times • Be respectful of other parents/carers and children • Direct any complaints or concerns through the Federation's official channels, so they can be dealt with in line with the Federation's complaints procedure I will not: • Use private groups, the Federation's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the Federation can't improve or address issues if they aren't raised in an appropriate way • Use private groups, the Federation's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the Federation 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 other children's parents/carers	
Signed:	**Date:**

Appendix 3: Acceptable use agreement for pupils

Acceptable use of the Federation's ICT facilities and internet: agreement for pupils and parents/carers	
Name of pupil:	
When I use the Federation's ICT facilities (like computers and equipment) and get on the internet in Federation, I will not: • Use them without asking a teacher first, or without a teacher in the room with me • Use them to break Federation 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 • Share my password with others or log in using someone else's name or password • Bully other people I understand that the Federation will check the websites I visit and how I use the Federation'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 a Federation computer or online that upsets me, or that I know is mean or wrong. I will always be responsible when I use the Federation's ICT systems and internet. I understand that the Federation can discipline me if I do certain unacceptable things online, even if I'm not in Federation when I do them.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the Federation's ICT systems and internet when appropriately supervised by a member of Federation staff. I agree to the conditions set out above for pupils using the Federation's ICT systems and internet, and for using personal electronic devices in Federation, 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 Federation's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the Federation's ICT facilities and accessing the internet in the Federation, or outside the Federation 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 Federation'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 Federation's network • Access my personal mobile telephone or other electronic communication devices teaching time (only during breaktimes and at lunchtime) • Access my personal mobile telephone and other electronic communication devices when in the proximity of the children and other service users • Allow my personal social media accounts to be linked to the Federation in any way • Have my social media accounts configured with open access (they should be set to private) or post any unprofessional comments, views or opinions. • Share my password with others or log in to the Federation's network using someone else's details • Share confidential information about the Federation, its pupils or staff, or other members of the community • Begin to use any new methods of collecting or storing personal or sensitive information- e.g. new apps which require input of pupils personal data without first seeking permission • 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 Federation • Delay in reporting any data breach as set out in the Federation's Data Protection Policy and breach procedure	
I understand that the Federation will monitor the websites I visit and my use of the Federation'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 Federation, and keep all data securely stored in accordance with this policy and the Federation's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil 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 Federation's ICT systems and internet responsibly, and ensure that pupils 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 Federation 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.
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.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like 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.

TERM	DEFINITION
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	Programs 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 executives.