ACCEPTABLE USE OF IT INTERNET AND ELECTRONIC COMMUNICATION POLICY

REVIEWED BY FGB

DATED : OCTOBER 2026

MINUTE NUMBER APPROVAL FGB 2189/2 OCTOBER 2026:

NEXT REVIEW DATE: OCTOBER 2027

ACCEPTABLE USE OF IT, INTERNET AND ELECTRONIC COMMUNICATION

This policy reflects the vision and aims of Hadfield Infant School.

Information and communications technology (IT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including the senior leadership team), governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school.
However, the IT resources and facilities our school uses could also pose risks to data protection, online safety and safeguarding. We are committed to using IT facilities in a way that meets legal requirements and upholds confidentiality and people's privacy rights. This policy aims to:

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

This policy covers all users of our school's IT facilities, including governors, staff, pupils, volunteers, contractors and visitors.
Breaches of this policy may be dealt with under our staff code of conduct.

ROLES AND RESPONSIBILITIES

Everyone who works for Hadfield Infant School has a responsibility to ensure that data is collected, accessed, stored and handled appropriately and lawfully. Every user must ensure that they adhere to this policy in order to meet the legal obligations of the school and their individual obligations.
The school's Board of Governors, whilst ultimately responsible for ensuring the school meets it legal obligations, is assisted directly by the senior leadership team.
Breaches of this policy should be reported to the Headteacher in the first instance.

DEFINITIONS

IT 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 school's IT service

Users: Anyone authorised by the school to use the school's IT facilities, including governors, staff, pupils, volunteers, contractors and visitors

Personal use: Any use of activity not directly related to the user's employment, study or purpose agreed by an authorised user

Authorised personnel: Employees authorised by the school to perform systems administration and/or monitoring of the IT facilities

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

Unacceptable use

The following is considered unacceptable use of the school's IT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings.

Unacceptable use of the school's facilities includes:

- Using the school's IT facilities to breach intellectual property rights or copyright
- Using the school's IT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies and 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 school or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's IT network without approval from authorised personnel
- Setting up any software, applications or web services on the school'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 school's IT 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 school's IT facilities
- Causing intentional damage to the school's IT facilities
- Removing, deleting or disposing of the school's IT 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 school
- Using websites or mechanisms to bypass the school's filtering and monitoring systems
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policy on behaviour and staff code of conduct.
Copies can be found on our school website and at our school office.

PUPILS

The following IT facilities are available to pupils in school:

- Computers, laptops and equipment are available in the classroom and are only available to pupils under supervision from members of staff.
- Specialist IT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff
- Pupils should only be able to access their DOJO avatar whilst under supervision from parents or staff

Under the Education Act 2011, the headteacher, and any member of staff authorised to do so by the headteacher, can search pupils 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 pupils **and/or**
- It is identified in the school's 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 and videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Before a search is conducted, authorised staff members (DSL) must be satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Assess how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

- Contact parents wherever feasible and possible to inform them of the situation should it be safe to do so (where the search does not relate to a safeguarding incident that involves parents/carers)

The authorised staff member should:

- Inform the DSL of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item.
- Involve the DSL 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 school 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 either the DSL or headteacher 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 possible. If the material is not suspected to be evidence in relation to an offence, staff members may delete if:

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

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 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 2024) on *sharing nudes and semi-nudes, advice for education settings working with children and young people*.

UNACCEPTABLE USE OF ICT AND THE INTERNET BY PUPILS OUTSIDE SCHOOL

The school will sanction pupils, in line with our Behaviour policy, if a pupil engages in any of the following **at any time:**

- Using IT or the internet to breach intellectual property rights or copyright
- Using IT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school'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 school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school 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 school's IT facilities
- Causing intentional damage to the school's IT 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

STAFF - INCLUDING GOVERNORS, VOLUNTEERS AND CONTRACTORS

The SBM and IT provider manages access to the school's IT facilities and materials for school 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 school's IT 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 Mel Wilkinson (SBM) or Rebecca Sutton (IT lead).

USE OF PHONES, EMAILS AND CLASS DOJO

The school 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 account(s). All work-related business should be conducted using the email address the school has provided.

Staff must **not** share their personal email addresses with parents/carers and pupils, and must not send any work-related materials using their personal email account. 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 and General Data Protection Act 2021 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. Alternatively documents can be sent via Perspective lite.

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 IT lead [Rebecca Sutton] immediately and follow our data breach procedure.

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

School 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

PERSONAL USE

Staff are permitted to occasionally use school IT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The IT lead /SBM/headteacher 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/teaching hours/non-break time]
- Does not constitute 'unacceptable use'
- 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 school's IT facilities to store personal, non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the school's IT facilities for personal use may put personal communications within the scope of the school's IT monitoring activities. Where breaches of this policy are found, disciplinary action may be taken.
Staff should be aware that personal use of IT (even when not using school IT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents/carers could see them.
Staff should take care to follow the school's guidelines on use of social media (see appendix 1 and **THE SCHOOLS SOCIAL MEDIA POLICY** [ON THE WEB SITE IN THE SAFEGUARDING SECTION] and use of email to protect themselves online and avoid compromising their professional integrity.

PERSONAL SOCIAL MEDIA ACCOUNTS

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times.
The school has guidelines for staff on appropriate security settings for Facebook Tik Tok Instagram X Snapchat and other accounts (see appendix 1).

REMOTE ACCESS

We allow staff to access the school's IT facilities and materials remotely. Staff accessing the school's IT 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 school's facilities outside the school and must take such precautions as the Headteacher may require against importing viruses and compromising system security.
Our IT 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.

FILTERING AND MONITORING OF THE SCHOOL NETWORK AND USE OF ITS FACILITIES

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its IT 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 IT personnel and SLT may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.
The school monitors IT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and IT operation
- Conduct training or quality control exercise

- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Our governing body is responsible for making sure that:

- The school 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

- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding lead (DSL) will take lead responsibility alongside our IT subject lead for understanding the filtering and monitoring systems and processes in place. Where appropriate, staff may raise concerns about monitored activity with the school's DSL and IT manager, as appropriate.

PARENTS/CARERS

Access to IT facilities and materials

Parents/carers do not have access to the school's IT facilities as a matter of course. However, parents/carers working for, or with, the school 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 school's facilities at the headteacher'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 school online

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

Communicating with parents/carers about pupil activity

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

In particular, staff will let parents/carers know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction. Parents/carers may seek any support and advice from the school to ensure a safe online environment is established for their child.

Communication via ClassDojo

ClassDojo is a new form of communication between staff and parents regarding events occurring in school. Please note that messages sent after 5pm will not be responded to until the next working day. Parents/Carers will be expected to abide by the same rules as above by communicating respectfully online both to staff and other parents. Misuse of ClassDojo will be reported as a safeguarding matter to the DSL and further action may be taken.

DATA SECURITY

The school 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 cybercrime technologies.
Staff, pupils, parents/carers and others who use the school's IT 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

Passwords

All users of the school's IT facilities should set strong passwords for their accounts and keep these passwords secure. 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, visitors or volunteers who disclose account or password information may have their access rights revoked.
All staff will use the password manager required by the network manager to help them store their passwords securely. Teachers will generate passwords for pupils using the required password manager or generator and keep these in a secure location in case pupils lose or forget their passwords.

Software updates, firewalls and anti-virus software

All of the school's IT 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 school's IT facilities.
Any personal devices using the school'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 school's data protection policy.
Our Data protection policy can be found on our school website. The disaster recovery plan is kept on the school server and a hard copy in the office.

Access to facilities and materials

All users of the school's IT facilities will have clearly defined access rights to school systems, files and devices.
These access rights are managed by our SBM and IT network manager.
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 our SBM and IT manager 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 school makes sure that its devices and systems have an appropriate level of encryption.
School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.
Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption.

PROTECTION FROM CYBER ATTACKS

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

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school'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 school will verify this using a third-party audit 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 school 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 OneDrive.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to IT Manager.
- 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 school email accounts
    - Store passwords securely using a password manager
- Make sure IT staff conduct regular access reviews to make sure each user in the school 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 school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident.
- Work with the Education Data Hub (who we subscribe to) at Derbyshire County Council regarding cyber security, such as advice on which service providers to use or assistance with procurement.

INTERNET ACCESS

The school's wireless internet connection is secure. We use filtering systems to ensure that the content provided to both staff, volunteers, governors and pupils is safe and monitor this on a regular basis.

Whilst we endeavour to ensure no material which could cause harm is available online through our filtering systems there are certain times when something may arise. If this occurs the member of staff will inform the Headteacher, DSL and IT Manager to ensure that this is included within the filtering systems in place.

Pupils

Pupils can access the Wi-Fi through the IT facilities provided such as computers and laptops. Filtering systems are in place on all devices within school. This will be monitored on a regular basis to ensure that there are no safeguarding risks to any pupil whilst accessing the internet through our Wi-Fi.

Parents/carers and visitors

Parents/carers and visitors to the school will not be permitted to use the school's Wi-Fi unless specific authorisation is granted by the headteacher.
The headteacher will only grant authorisation if:

- Parents/carers are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school's Wi-Fi 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 Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

MONITORING AND REVIEW

The headteacher, IT Manager and SBM will monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.
This policy will be reviewed every year. The governing board is responsible for reviewing/approving this policy.

Do not accept friend requests from pupils on social media

APPENDIX 1: Social Media [Facebook Tik Tok Instagram X Snapchat] cheat sheet for staff

10 rules for school 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 pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or pupils)

Check your privacy settings

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

A pupil adds you on social media

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

A parent/carer adds you on social media

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

- Responding to 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the school
- Pupils may then have indirect access through their parent/carer's account to anything you post, share, comment on or are tagged in

If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent/carer know that you're doing so

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

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or 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 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 school. The school uses the following channels: • Our Office Facebook Page • E-mail groups for parents and text alerts • Class Dojo 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 school via official communication channels, or using private/independent channels to talk about the school, I will: • Be respectful towards members of staff, and the school, at all times • Be respectful of other parents/carers and children • Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure I will not: • Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues unless they are raised in an appropriate way • Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school 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	
Signed:	**Date:**

APPENDIX 3: Acceptable use agreement for older pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers	
Name of pupil:	
When using the school's ICT facilities and accessing the internet in school, I will not: • Use them for a non-educational purpose • Use them without a teacher being present, or without a teacher's permission • Use them to break school rules • Access any inappropriate websites • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) • Use chat rooms • 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 • Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo/video • Share my password with others or log in to the school's network using someone else's details • Bully other people I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the school's ICT systems and internet responsibly. I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

APPENDIX 4: Acceptable use agreement for younger pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers	
Name of pupil:	
When I use the school's ICT facilities (like computers and equipment) and go on the internet in school, I will not: • Use them without asking a teacher first, or without a teacher in the room with me • Use them to break school 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 I understand that the school will check the websites I visit and how I use the school'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 school computer or online that upsets me, or that I know is mean or wrong. I will always be responsible when I use the school's ICT systems and internet. I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

APPENDIX 5: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT facilities and accessing the internet in school, or outside school 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 school'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 school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school, its pupils 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 school

I understand that the school will monitor the websites I visit and my use of the school'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 school, and keep all data securely stored in accordance with this policy and the school'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 school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

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

APPENDIX 6: Glossary of cyber security terminology

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.

Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.

This list is not extensive and is constantly changing