Queen's Park Mission Statement
Bravely navigate a changing world—with curiosity, confidence, and joy.
Queen's Park Vision
Our children love coming to school. They experience success through strong, trusting relationships, a deep sense of belonging, positive connections with others, and the courage to challenge themselves.
We celebrate the strength of our diverse community. We create a safe, welcoming environment where every child is seen, heard, and truly valued. Learning is exciting and challenging, with plenty of opportunities to explore new ideas, aim high, and discover individual talents.
We encourage children to ask big questions, stand up for what they believe, and understand different perspectives.
Together with families, we help children develop the knowledge, skills, and character they need to thrive in a changing world. We want every child to feel proud of who they are—and brave enough to shape a better future.
Queen's Park Values
Kindness - Integrity - Excellence - Collaboration

ICT and Internet Acceptable Usage Policy

Date	July 2025
Review Date	July 2026

Contents

---

1. Introduction and aims

Information and communications technology (ICT) 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 ICT resources and facilities our school uses could also pose risks to data protection, online safety and safeguarding.

This policy aims to:

> Set guidelines and rules on the use of school ICT 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 ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our school disciplinary procedures.

2. Relevant legislation and guidance

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

- Data Protection Act 2018

- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020

- Computer Misuse Act 1990

- Human Rights Act 1998

- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

- Education Act 2011

- Freedom of Information Act 2000

- Education and Inspections Act 2006

- Keeping Children Safe in Education 2023

- Searching, screening and confiscation: advice for schools 2022

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

- Education and Training (Welfare of Children) Act 2021

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

- Meeting digital and technology standards in schools and colleges

3. Definitions

- **ICT facilities:** 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 ICT service

- **Users:** anyone authorised by the school to use the school's 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 agreed by an authorised user

- **Authorised personnel:** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities

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

See appendix 4 for a glossary of cyber security terminology.

4. Unacceptable use

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

> Using the school's ICT facilities to breach intellectual property rights or copyright

> Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination

> Breaching the school'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 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 ICT 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 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 school's ICT facilities

> Causing intentional damage to the school's ICT facilities

> Removing, deleting or disposing of the school's ICT equipment, systems, programmes, information, files or data 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 or monitoring mechanisms

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

> Using AI tools and generative chatbots to write homework or present AI-generated work as their own

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

4.1 Exceptions from unacceptable use

Where the use of school ICT facilities (on the school 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 headteacher's discretion. For example, the use of AI tools or generative chatbots for the purpose of learning about their function and uses.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies on behaviour and staff conduct.

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

5.1 Access to school ICT facilities and materials

The school business manager manages access to the school's ICT 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 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 school business manager.

5.1.1 Use of phones and email

The school provides each member of staff with an email address.
This email account should be used for work purposes only. Once installed, staff will use multi-factor authentication on their email 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 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 will be automatically encrypted

within the local authority or manually encrypted outside of the local authority 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 school business manager and follow our data breach procedure.

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

School phones must not be used for personal matters unless meeting a permitted exception (see below 5.2 Personal Use).

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 school may record incoming and outgoing phone conversations for training and monitoring purposes.

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused.

Personal use is permitted provided that such use:

> Does not take place during teaching time

> 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 school'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 school's ICT facilities for personal use may put personal communications within the scope of the school'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 school's usage policy.

Staff should be aware that personal use of ICT (even when not using school ICT 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 below 5.2.1 personal social media accounts) 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 make sure their use of social media, either for work or personal purposes, is appropriate at all times.

It is recommended that staff regularly check the security settings for their social media accounts.

5.3 Remote access

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

> Will need to explain who manages, security, protocols

Staff accessing the school'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 school's ICT facilities outside the school and must take such precautions as directed by the school to prevent 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.

5.4 School social media accounts
The school has an official Facebook and Instagram account, managed by the headteacher.
The school has guidelines for what may and must not be posted on its social media accounts.

5.5 Monitoring and filtering of the school network and use of ICT 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 ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

> Internet sites visited

> Bandwidth usage

> Email accounts

> Telephone calls

> User activity/access logs

> Any other electronic communications

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. Queen's Park Primary uses the Smoothwall filtering system. This is set up and managed by Schools ICT Support in line with other Brighton & Hove Maintained Primary Schools. Alerts generated by Smoothwall are monitored by the headteacher and Schools ICT Support.

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

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

6. Pupils

6.1 Access to ICT facilities

Children have access to a variety of ICT favilities at Queen's Park Primary:
> Children will have supervised access to tablets, laptops and computers in order to meet their curriculum needs

> KS1 pupils will use generic year group log ins to access the school computers.

> KS2 pupils will use personal network log ins and passwords to access the school computers.

> KS2 children will use their school Google account to access our Chromebook laptops

6.2 Search and deletion

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**

> Is identified in the school 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:
> Make an assessment of 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 or DSL.

> 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 whenever possible or follow the procedure as laid out in the school behaviour policy

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 (or deputy) without delay if they believe that a search has revealed a safeguarding risk

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

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

> Cause harm, **and/or**

> Undermine the safe environment of the school or disrupt teaching, **and/or**

> Commit an offence

If inappropriate material is found on the device, it is up to headteacher or DSL 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 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 (or DDSL) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

> The DfE's latest guidance on searching, screening and confiscation

> UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

> Our behaviour policy and child protection and safeguarding policies

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

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour and online safety policies, if a pupil engages in any of the following **at any time** (even if they are not on school 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 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 ICT facilities

> Causing intentional damage to the school's ICT facilities or materials

> Causing a data breach by accessing, modifying, sharing or deleting files or data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation

> Using inappropriate or offensive language

7. Parents/carers

7.1 Access to ICT facilities and materials

Parents/carers do not have access to the school's ICT 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.

7.2 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.
We ask parents/carers to sign the appropriate agreements laid out in appendices 1-3.

7.3 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.

8. 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 cyber crime technologies.

Staff, pupils, parents/carers and others who use the school'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 some or all of the following:

> Firewalls

> Security features

> User authentication and multi-factor authentication

> Anti-malware software

8.1 Passwords

All users of the school's ICT 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.

The ICT Technician or Schools ICT Support will generate passwords for pupils and work with the Computing Coordinator to keep these in a secure location in case pupils lose or forget their passwords.

8.2 Software updates, firewalls and anti-virus software

All of the school'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 by the ICT Technician, ICT Consultant or School's ICT Support.

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 ICT facilities.

Any personal devices using the school'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 school's data protection policy.

8.4 Access to facilities and materials

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

These access rights are managed by the School Business Mananger.

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 School Business 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.

8.5 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, as defined by the ICT Technician, ICT Consultant or School's ICT Support.

9. Protection from cyber attacks

Please see the glossary (appendix 4) to help you understand cyber security terminology.

The school will:

- Work with governors and School's ICT Support 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 (such as 360 degree safe) 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 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 daily and store these backups on our server and backed up on local authority servers.

> Delegate specific responsibility for maintaining the security of our management information system (MIS) to school business manager and Schools ICT Support

> 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

> Make sure school business manager 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 School's ICT Support 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. This plan will be reviewed and tested by Schools ICT Support and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

> Work with School's ICT Support to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement

10. Internet access

The school's wireless internet connection is secure. Queen's Park Primary uses the Smoothwall filtering system. This is set up and managed by Schools ICT Support in line with other Brighton & Hove Maintained Primary Schools. Alerts generated by Smoothwall are monitored by the headteacher and Schools ICT Support. Actions will be taken as deemed appropriate by the headteacher.

10.1 Pupils

Children have supervised access to the internet by Wifi. This is available on tablets, laptops and computers. The Smoothwall filtering system is used to safeguard children whilst using these devices. Access to the internet is provided in line with the conditions outlined in this policy.

10.2 Parents/carers and visitors
Parents/carers and visitors to the school will not be permitted to use the school's WiFi 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 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 headteacher and Computing Coordinator 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 approving this policy annually.

12. Related policies

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

- Online safety

- Code of conduct for parents/carers

- Safeguarding and child protection

- Behaviour

- Staff discipline

- Data protection

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

When I use the school's ICT systems (like tablets and computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
  - I select a website by mistake
  - I receive messages from people I don't know
  - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

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 will make sure my child understands these.

Signed (parent/carer):	Date:

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy.

When I use the school's ICT systems (like tablet, laptops and computers) and get onto the internet in school I will:

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

I will not:

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

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

- I will hand it to my teacher when I arrive at school

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):	Date:

Parent/carer's 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 3: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET:

AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

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

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way that 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
- Use photographs of pupils without first checking the permissions excel spreadsheet
- 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 private businesses, unless that business is directly related to the school

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

I agree 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 technician and ICT consultant know if a pupil informs me they have found any material that 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 4: Glossary of cyber security terminology

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

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

TERM	DEFINITION
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 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.