Harrietsham Church of England Primary School

ICT Acceptable Use Policy

Policy lead:	Jackie Chambers
Responsibility:	Headteacher
Date approved by Governing Body:	September 2025
Governor signature:	Rebecca Emson (Chair)
Review date:	September 2026

Harrietsham Church of England Primary School

ICT Acceptable Use Policy

Contents

School Context: 3

1. Introduction and aims 3
2. Relevant legislation and guidance 4
3. Definitions 4
4. Unacceptable use....4
5. Staff (including governors, volunteers, and contractors) 5
6. Pupils 8
7. Parents/carers 10
8. Data security 10
9. Protection from cyber attacks 11
10. Internet access 12
11. Monitoring and review 13
12. Related policies 13

Appendix 1: Facebook cheat sheet for staff. 14
Appendix 2: Acceptable use of the internet: agreement for parents and carers. 15
Appendix 3: Acceptable use agreement for older pupils (Key Stage 2). 18
Appendix 4: Acceptable use agreement for younger pupils (EYFS and Key Stage 1). 21
Appendix 5: Acceptable use agreement for staff. 23
Appendix 6: Acceptable use agreement for Governors, volunteers and visitors. 27
Appendix 7: Wi-Fi Acceptable Use Policy. 28
Appendix 8: PTFA and Forest School Social Networking Acceptable Use Policy. 29
Appendix 9: Glossary of cyber security terminology. 30

School Context:

Harrietsham CEP Vision Statement

We are a warm, welcoming, and inclusive school rooted in our rural community. Like the mustard seed we grew from tiny beginnings and our branches are now spread wide –providing support and taking our values beyond the school gates. All those in our community feel safe and nurtured - able to flourish and grow academically, spiritually, emotionally and physically to achieve their full God-given potential.

"Nurtured we flourish"

We are a nurturing school. As such we believe in, and follow, **The Six Principles of Nurture** in all of our practice.

1. Children's learning is understood developmentally.
2. The classroom offers a safe base.
3. The importance of nurture for the development of wellbeing.
4. Language is a vital means of communication.
5. All behaviour is communication.
6. The importance of transition in children's lives.

Our Values

The roots of our vision are in the parable of the Mustard Seed.

'The kingdom of heaven is like a mustard seed, which a man took and planted in his field. Though it is the smallest of all seeds, yet when it grows, it is the largest of garden plants and becomes a tree, so that the birds come and perch in its branches'.
Matthew 13 31-32

In order to grow and reach our potential, everything that we do in school is driven by our vision and underpinned by our core Christian values of:

Love, Fellowship and Forgiveness

---

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 staff disciplinary policy, behaviour policy, staff behaviour policy, staff code of conduct.

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 9** 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 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 or monitoring mechanisms.
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way.
- Using AI tools and generative chatbots (such as ChatGPT and Google Bard) where AI-generated text or imagery is presented as your own work.

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 Headteachers discretion.

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, staff behaviour, staff code of conduct. Sanctions could include revoking permission to use the school's systems.

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

5.1 Access to school ICT facilities and materials

The school's Business Leader 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 Business Leader.

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. Staff should enable 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 should be encrypted so that the information is only accessible by the intended recipient.

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

If staff send an email in error that contains the personal information of another person, they must inform the Business Leader 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. The exception to this is Senior Leaders who may use their personal mobile phones to communicate with Governors, the PTFA or volunteers about work related issues or with parents in case of emergencies.

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 as set out in section 4.

The school can record incoming and outgoing phone conversations.

If you record calls, callers **must** be made aware that the conversation is being recorded and the reasons for doing so.

Staff who would like to record a phone conversation should speak to the Headteacher.

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

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. The Business Leader 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 with the children.
- 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 mobile phone and smart technology 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 **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 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 accounts (see **Appendix 1**).

5.3 Remote access

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

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 the Business Leader may require against importing viruses or compromising system security.

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

5.4 School social media accounts

The school has official OPAL and Forest School social media accounts, managed by the OPAL Leader and the Forest School Specialist. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

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

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.

The school monitors ICT use in order to:

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

Our governing board 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 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 Business Leader, as appropriate.

6. Pupils

6.1 Access to ICT facilities

- Any ICT equipment (such as computers, laptops and i-pads / tablets, etc) are available to pupils only under the supervision of staff.
- Specialist ICT equipment, such as that used for music, or design and technology, will only be used under the supervision of staff.

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 in order to confiscate an item, 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.
- 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.

The authorised staff member should:

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

Any searching of 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.

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 Policy, 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, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation.
- Using inappropriate or offensive language.

7. Parents/carers

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 agreement in **Appendix 2.**

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 Home Learning 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 cybercrime 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:

- 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.

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.

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.

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 Business Leader.

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 Business Leader 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 Business Leader.

9. Protection from cyber attacks

Please see the glossary (**Appendix 9**) 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* (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 cloud-based backup systems.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our cloud-based provider.
- Make sure staff:
    - Dial into our network using a virtual private network (VPN) when working from home.
    - Enable multi-factor authentication where they can, on things like school email accounts.
    - Store passwords securely using a password manager.
- Make sure ICT 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. This plan will be reviewed and tested annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'.
- Work with our LA 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.

Our WiFi is filtered.

We are aware that filters aren't foolproof. Any inappropriate sites that the filter hasn't identified (or appropriate sites that have been filtered in error) should be reported to the DSL (or deputy) if they present a safeguarding concern and the schools ICT provider.

10.1 Pupils

Our children can access WiFi only under the direct supervision of staff. Any content searched online with will filtered.

If a child has a concern that something has not been filtered, they are taught to close their screen immediately and tell a staff member.

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 Business Leader 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 and approving this policy.

12. Related policies

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

- Online Safety
- Safeguarding and Child Protection
- Behaviour
- Staff Behaviour (Code of Conduct)
- Data Protection (GDPR)
- Remote Education
- Mobile Phone and Smart Technology

Appendix 1: Facebook cheat sheet for staff.

Do not accept friend requests from pupils on social media

10 rules for school staff on Facebook

1. Make sure your display name is professional – consider using your first and middle name, using a maiden name, or putting 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.

What to do 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/carers. If the pupil persists, take a screenshot of their request and any accompanying messages – do not reply to the student online.
- 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.

Dear Parent/Carer,

All pupils at Harrietsham Church of England Primary School use computer facilities and internet access as an essential part of learning as required by the National Curriculum. Your child will have the opportunity to access a wide range of information and communication technology (ICT) resources.

This includes access to:

- Laptops, tablets and other digital devices.
- The Internet, which may include search engines and educational sites.
- School learning platform/intranet.
- Email.
- Digital cameras, webcams and video cameras.

Harrietsham Church of England Primary School recognises the essential and important contribution that technology plays in promoting children's learning and development and believes it offers a fantastic range of positive activities and experiences. We do recognise, however, that this can bring risks. We take your child's online safety seriously and, as such, will take all reasonable precautions, including monitoring and filtering systems, to ensure that pupils are safe when they use our internet and systems.

We recognise, however, that no technical system can replace online safety education and believe that children themselves have an important role to play in developing responsible behaviour. To support the school in developing your child's knowledge and understanding about online safety, we request that you read the attached Acceptable Use Policy with your child, discuss the content with them and return the attached slip. There is a copy for you and two copies for children – one for Key Stage Two children and one for EYFS and Key Stage One children.

We understand that your child in EYFS is too young to give informed consent on his/ her own; however, we feel it is good practice to involve them as much as possible and believe a shared commitment is the most successful way to achieve this.

Hopefully, you will find this Acceptable Use Policy provides you with an opportunity for conversations between you and your child about safe and appropriate use of the technology, both at school and at home. All parents/carers are required to follow this policy as part of being a responsible member of our wider school community.

We request that all parents support our approach to online safety by role modelling safe and positive online behaviour and by discussing online safety whenever children access technology at home. Parents can visit the school website (www.harrietsham.kent.sch.uk) for more information about our approach to online safety.

Full details of the school's online safety policy are available on the school website or on request. Parents/carers may also like to visit the following links for more information about keeping children safe online:

- www.thinkuknow.co.uk
- www.childnet.com
- www.nspcc.org.uk/onlinesafety
- www.saferinternet.org.uk
- www.internetmatters.org

Should you wish to discuss the matter further, please do not hesitate to contact a member of the Senior Leadership Team or the Designated Safeguarding Lead (Mrs Griffin).

Yours sincerely,

Mrs Jackie Chambers
Headteacher

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 OPAL and Forest School Facebook page (OPAL Tik Tok / Instagram pages)
- Email / text groups for parents (for school announcements and information)
- Dojo
- Our website

Parents/carers sometimes also set up independent channels to help them stay on top of what's happening in their child's class. For example, 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 OPAL or Forest School 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 pages, 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.

My Child's use of ICT:

- I have read and discussed Harrietsham Church of England Primary School Learner Acceptable Use Policy with my child and understand that it will help keep my child safe online.
- I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet, both in and out of school.
- I understand that the Acceptable Use Policy applies to my child's use of school devices and systems on site and at home, and personal use where there are safeguarding and/or behaviour concerns. This may include if online behaviour poses a threat or causes harm to another child, could have repercussions for the orderly running of the school, if a child is identifiable as a member of the school or if the behaviour could adversely affect the reputation of the school.
- I am aware that any internet and computer use using school equipment may be monitored for safety and security reasons, to safeguard both my child and the schools' systems. This monitoring will take place in accordance with data protection (including GDPR) and human rights legislation.
- I am aware that my child (unless they are on Year 6) cannot bring personal devices and mobile technology on site. Year 6 pupils are required to hand their mobile phone to their teacher as soon as they enter site. These

phones are then locked away until the end of the school day, when they are redistributed as pupils leave the site.

- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- I understand that if the school has any concerns about my child's safety online, either at school or at home, then I will be contacted.
- I understand that if my child does not abide by the school Acceptable Use Policy inside or outside of school, then sanctions will be applied in line with the school policies including behaviour, online safety and anti-bullying policy. If the school believes that my child has committed a criminal offence then the Police will be contacted.
- I, together with my child, will support the school's approach to online safety and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community or content that could adversely affect the reputation of the school.
- I know that I can speak to the school Designated Safeguarding Lead, my child's teacher or a member of the senior leadership team if I have any concerns about online safety.
- I understand that my child may need a safe and appropriate place to access Home learning. I will ensure my child's access to remote/online learning is appropriately supervised and any use is in accordance with the school's ICT Acceptable Use Policy. If accessing video learning, I will ensure they are in an appropriate location (e.g. not in bed) and that they are suitably dressed and that they are supervised.
- I understand my role and responsibility in supporting the school's online safety approaches and safeguarding my child online. I will use parental controls, supervise access and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding
- I will visit the school website www.harrietsham.kent.sch.uk for more information about the school's approach to online safety as well as to access useful links to support both myself and my child in keeping safe online at home.
- I will visit the following websites for more information about keeping my child(ren) safe online:
    - www.thinkuknow.co.uk/parents,
    - www.nspcc.org.uk/onlinesafety
    - www.internetmatters.org
    - www.saferinternet.org.uk
    - www.childnet.com
- I will support the school and my child by role modelling safe and positive online behaviour (such as sharing images, text and video responsibly) and by discussing online safety with them when they access technology at home.

Signed:	**Date:**

Appendix 3: Acceptable use agreement for older pupils (Key Stage 2).

Dear Children,

All children at our school use computer facilities, including internet access, as an essential part of learning in today's modern British Society. You will have the opportunity to access a wide range of technology resources.

This includes access to:

- Laptops, tablets and other digital devices.
- The internet, which may include search engines and educational sites.
- School learning platform/intranet.
- Email.
- Games consoles and other games-based technologies.
- Digital cameras, webcams and video cameras.

At Harrietsham Church of England Primary School we recognise the essential and important contribution that technology plays in promoting your learning and development, both at school and at home. However, we also recognise there are potential risks. The school will take all reasonable precautions to ensure that you are as safe as possible when using school equipment and will work together with you and your family to help you stay safe online.

At Harrietsham Church of England Primary School we want to ensure that all members of our community are safe and responsible users of technology.

We will support you to:

- Become empowered and responsible digital creators and users.
- Use our resources and technology safely, carefully and responsibly.
- Be kind online and help us to create a community that is respectful and caring, on and offline.
- Be safe and sensible online, and always know that you can talk to a trusted adult if you need help.

Should you have any worries about online safety, you can speak with your class teacher or any other adult in school. You can also access support via other websites such as www.thinkuknow.co.uk and www.childline.org.uk.

As a member of our school community you must follow the rules laid out in our acceptable use policy for learners below. Please sign and return the agreement to your teacher.

We look forward to helping you become a positive and responsible digital citizen.

Yours sincerely,

Mrs Jackie Chambers
Headteacher

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers (Key Stage 2):

Name of pupil:

When using the school's ICT facilities and accessing the internet in school:

Safe

- I will behave online as I am expected to behave in the classroom.
- I only send messages which are polite and friendly.
- I will only post pictures or videos on the internet if they are appropriate and if I have permission.
- I only talk with and open messages from people I know.
- I will only click on links if I know they are safe.
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult.

Learning

- I will save learning in the correct area and will ask my teacher if I'm not sure where to save.
- I will not use my own personal devices in school.
- I always ask permission from an adult before using the internet.
- I only use websites and search engines that my teacher has chosen.
- If I need to learn online at home, I will follow this policy.

Trust

- I know that not everything or everyone online is honest or truthful.
- I will check content on other sources like other websites, books or with a trusted adult.
- I always credit the person or source that created any work, image or text I use.

Responsible

- I only use school computers for school learning, unless I have permission otherwise.
- I keep my personal information safe and private online.
- I will keep my passwords safe and not share them with anyone.
- I will not access or change other people's files or information.

Understand

- I understand that the school's internet filter is there to protect me, and I will not try to bypass it.
- I know that my use of school devices, computers and internet access will be monitored.
- I have read and talked about these rules with my parents/carers.
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about keeping safe online.
- I know that if I do not follow the school rules, I will be sent to the Headteacher.

Tell

- If I am aware of anyone being unsafe with technology, I will report it to a teacher.

- I always talk to an adult if I'm not sure about something or if something happens online that makes me feel worried or frightened.
- If I see anything online that I shouldn't or that makes me feel worried or upset, I will shut the laptop lid and tell an adult straight away.
- I know that I will be able to use the internet in school, for a variety of reasons, if I use it responsibly. However, I understand that if I do not, I may not be allowed to use the internet at school.
- I know that being responsible means that I should not look for bad language, inappropriate images or violent or unsuitable games, and that if I accidently come across any of these I should report it to a teacher or adult in school or a parent or carer at home.
- I will treat my password like my toothbrush! This means I will not share it with anyone (even my best friend), and I will log off when I have finished using the computer or device.
- I will protect myself by never telling anyone I meet online my address, my telephone number, my school's name or by sending a picture of myself without permission from a teacher or other adult.
- I will never arrange to meet anyone I have met online alone in person without talking to a trusted adult.
- If I get unpleasant, rude or bullying emails or messages, I will report them to a teacher or another trusted adult. I will not delete them straight away, but instead, keep them so I can show them to the person I am reporting it to.
- I will always be myself and not pretend to be anyone or anything I am not. I know that posting anonymous messages or pretending to be someone else is not allowed.
- I will always check before I download software or data from the internet. I know that information on the internet may not be reliable and it sometimes needs checking.
- I will be polite and sensible when I message people online and I know that sending a message is the same as having a conversation with someone. I will not be rude or hurt someone's feelings online.
- I know that I am not allowed on personal email, social networking sites or instant messaging in school.
- If, for any reason, I need to bring my mobile phone into school I know that it is to be handed in to the teacher and then collected at the end of the school day.
- I will tell a teacher or other adult if someone online makes me feel uncomfortable or worried when I am online using games or other websites or apps.
- If I bring in memory sticks / CDs from outside of school, I will always give them to my teacher so they can be checked for viruses and content before opening 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 (EYFS and Key Stage 1).

Dear Children,

All children at our school use computers and the internet to help them with their learning.

You will have the opportunity to access a wide range of technology resources, including:

- Laptops, tablets and other digital devices.
- The internet, which may include search engines and educational sites.
- School learning platform/intranet.
- Email.
- Games consoles and other games-based technologies.
- Digital cameras, webcams and video cameras.

At Harrietsham Church of England Primary School we want you to learn using computers and the internet, both at school and at home. However, we recognise there are potential risks if it is not used safely.

We will work hard to ensure that you are as safe as possible when using school equipment and will work together with you and your family to help you stay safe online.

At Harrietsham Church of England Primary School we want to ensure that all members of our community are safe and responsible users of technology.

We will support you to:

- Become safe digital creators and users.
- Use our resources and technology safely, carefully and responsibly.
- Be kind online and help us to create a community that is respectful and caring, on and offline.
- Be safe and sensible online, and always know that you can talk to a trusted adult if you need help.

Should you have any worries about online safety, you can speak with your class teacher or any other adult in school. You can also access support via other websites such as www.thinkuknow.co.uk and www.childline.org.uk.

As a member of our school community you must follow the rules laid out in our acceptable use policy for learners below. Please sign and return the agreement to your teacher.

We look forward to helping you become a positive and responsible digital citizen.

Yours sincerely,

Mrs Jackie Chambers
Headteacher

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers (EYFS and Key Stage 1):	
Name of pupil:	
When I use the school's ICT facilities (like computers and equipment) and go on the internet in school: • I only use the internet when an adult is with me. • I only click on links and buttons online when I know what they do. If I am not sure, I will ask an adult first. • I keep my personal information and passwords safe online. • I only send messages online which are polite and friendly. • I know the school can see what I am doing online when I use school computers or devices. This is so that they can help keep me safe and make sure I'm following the rules. • I know that if I do not follow the rules, I will be sent to the Headteacher. • I have read and talked about these rules with my parents/carers. • I always tell an adult/teacher if something online makes me feel upset, unhappy or worried. • I can visit www.thinkuknow.co.uk to learn more about keeping safe online. I will always be responsible when I use the school's computers 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.

Dear Staff,

At Harrietsham C of E Primary School we recognise that staff can be vulnerable to online risks. Social media can blur the definitions of personal and working lives; it is important that all members of staff at Harrietsham C of E Primary School take precautions to protect themselves both professionally and personally online.

We request that all members of staff:

- Are conscious of their own professional reputation and that of the school when online.
    - All members of staff are strongly advised in their own interests to take steps to ensure that their personal information and content is not accessible to anybody who does not or should not have permission to access it.
    - Content shared online cannot be guaranteed to be "private" and could potentially be seen by unintended audiences. This could have consequences including civil, legal and disciplinary action being taken.

- Are aware that as professionals, we must ensure that the content we post online does not bring the school or our professional role into disrepute and does not undermine professional confidence in our abilities.
    - The teaching standards state that as professionals we should be achieving the highest possible standards in our conduct, act with honesty and integrity and forge positive professional relationships.

- Are careful when publishing any information, personal contact details, video or images online.
    - It is very important to be aware that sometimes content shared online, even in jest, can be misread, misinterpreted or taken out of context, which can lead to complaints or allegations being made. Don't be afraid to be yourself online but do so respectfully.
    - Ensure that the privacy settings of the social media sites you use are set appropriately.
    - Consider if you would feel comfortable about a current or prospective employer, colleague, and child in your care or their parent/carer, viewing or sharing your content. If the answer is no, consider if it should be posted online at all.

- Not accept pupils (past or present) or their parents/carers as "friends" on a personal account.
    - You may be giving them access to your personal information and allowing them to contact you inappropriately through unregulated channels. They may also be giving you access to their personal information and activities which could cause safeguarding concerns.
    - If you have a pre-existing relationship with a child or parent/carer or any other situation that may compromise this, speak to the Designated Safeguarding Lead.

- Always use a work provided email address or phone number to contact children and parents – this is essential to protect yourself as well as the wider community.

- If you are concerned about a child's wellbeing or online behaviour, please speak to the Designated Safeguarding Lead. If you are targeted online by a member of the community or are concerned about a colleague, then please speak to a member of the senior leadership team.
    - If you are unhappy with the response you receive, you should escalate this by speaking to the Headteacher or Chair of Governors and if you are still not satisfied with the response then we request you follow our whistleblowing procedure.

- If you have any questions regarding online conduct expected of staff, please speak to the Designated Safeguarding Lead or Headteacher.

Documents called “Cyberbullying: Supporting School Staff”, “Cyberbullying: advice for headteachers and school staff” and “Safer professional practise with technology” are available in on the staff shared drive to help you consider how to protect yourself online.

Please print them if you want or download the documents directly from:

- www.childnet.com/teachers-and-professionals/for-you-as-a-professional
- www.gov.uk/government/publications/preventing-and-tackling-bullying
- www.saferinternet.org.uk
- www.kscb.org.uk/guidance/online-safety

Additional advice and guidance for professionals is available locally through the Education Safeguarding Team or nationally through Professional Unions and/or the Professional Online Safety helpline www.saferinternet.org.uk/about/helpline

I would like to remind all staff of our Acceptable Use Policy and the importance of maintaining professional boundaries online. Failure to follow this guidance and the school code of conduct could lead to disciplinary action; it is crucial that all staff understand how to protect themselves online.

Please speak to your line manager, the Designated Safeguarding Lead or myself if you have any queries or concerns regarding this.

Yours sincerely,

Mrs Jackie Chambers
Headteacher

Acceptable use of the school's ICT facilities and the internet: agreement for staff.

Name of staff member:

As a professional organisation with responsibility for safeguarding, it is important that staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using technology, they are asked to read and sign this Acceptable Use Policy.

Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the AUP will help ensure that all staff understand Harrietsham C of E school's expectations regarding safe and responsible technology use, and can manage the potential risks posed. The AUP will also help to ensure that school systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

This is not an exhaustive list; all members of staff are reminded that ICT use should be consistent with the school ethos, school policies, national/local guidance and expectations, and the Law.

1. I understand that Information Systems and IT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites**.**
2. I understand that Harrietsham C of E's Acceptable Use of Technology policy (AUP) should be read and followed in line with the staff Code of Conduct.
3. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
4. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate. I will protect the devices in my care from unapproved access or theft.
5. I will respect system security and will not disclose any password or security information. I will use a 'strong' password to access school systems. A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system.
6. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
7. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection legislation (including GDPR).
    - This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
    - Any data being removed from the school site (such as via email or on memory sticks) will be suitably protected. This may include data being encrypted by a method approved by the school.
    - Any images or videos of pupils will only be used as stated in the school image use policy and will always reflect parental consent.
8. I will not keep documents which contain school-related sensitive or personal information, including images, files, videos and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the School Learning Platform to upload any work documents and files in a password protected environment.
9. I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.
10. I will respect copyright and intellectual property rights.
11. I have read and understood the school online safety policy which covers the requirements for safe IT use, including using appropriate devices, safe use of social media and the supervision of pupils within the classroom and other working spaces.
12. I will immediately report any illegal, inappropriate or harmful material or incidents I become aware of, to the Designated Safeguarding Lead and Senior Leadership Team.

13. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, I will report this to the ICT Support Provider as soon as possible.
14. My electronic communications with current or past pupils, parents/carers and other professionals will take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
    - All communication will take place via school approved communication channels, such as a school provided email address or telephone number, and not via my personal devices or communication channels, such as personal email, social networking or mobile phones.
    - Any pre-existing relationships or situations that may compromise this will be discussed with the Designated Safeguarding Lead and Headteacher.
15. I will ensure that my online reputation and use of IT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, and gaming and any other devices or websites.
    - I will take appropriate steps to protect myself online as outlined in the **Online Safety Policy** and will ensure that my use of IT and the internet will not undermine my professional role, interfere with my work duties and will be in accordance with the **School Code of Conduct** and the Law.
16. I will not create, transmit, display, publish or forward any material online that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.
17. I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.
18. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school into disrepute.
19. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
20. If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the Designated Safeguarding Lead and the Headteacher.
21. I understand that my use of the school information systems, including any devices provided by the school, including the school internet and school email, may be monitored and recorded to ensure the safety of children and staff and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.
22. I understand that the school may exercise its right to monitor the use of information systems, including internet access and the interception of emails, to monitor policy compliance. Where it believes unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour, including that which may bring the reputation of the school into disrepute, may be taking place, the school may invoke its disciplinary procedures. If the school suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation.
23. Where I deliver or support remote learning, I will comply with this policy.
24. I have read and understood the school's policy for use of mobile phones.

Remote Learning

- Remote learning will take place using Class Dojo.
- Staff will use work provided equipment where possible.
- Online contact with learners / parents or carers should be available between 8.30am-4.30pm. Any messages received or sent after this time may not receive a response until the next working day.
- Any personal data used by staff when delivering remote learning will be processed and stored with appropriate consent and in line with our data protection policy.
- All remote learning and other online communication will take place in line with current school confidentiality expectations as outlined in our Staff Conduct and Discipline Policy.
- Only members of Harrietsham CE Primary school community will be given access to Class Dojo.
- Access to Class Dojo will be managed in line with current IT security expectations as outlined in this policy.

Signed (staff member):	**Date:**

Appendix 6: Acceptable use agreement for Governors, volunteers and visitors.

Acceptable use of the school's ICT facilities and the internet: agreement for Governors, volunteers and visitors.	
Name of Governor, volunteer or visitor:	

As a professional organisation with responsibility for children's safeguarding it is important that all members of the community, including visitors and volunteers, are fully aware of their professional responsibilities and read and sign this Acceptable Use Policy.

This is not an exhaustive list; visitors/volunteers are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

1. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with Data Protection legislation, including GDPR. Any data which is being removed from the school site, such as via email or on memory sticks or CDs, will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school image use policy and will always reflect parental consent.
2. I have read and understood the school online safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.
3. I will follow the school's policy regarding confidentially, data protection and use of images and will abide with copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.
4. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
    - All communication will take place via school approved communication channels such as via a school provided email address or telephone number and not via personal devices or communication channels such as via personal email, social networking or mobile phones.
    - Any pre-existing relationships or situations that may compromise this will be discussed with the Designated Safeguarding Lead and/or Headteacher.
5. My use of ICT and information systems will be compatible with my role within school. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. I will take appropriate steps to protect myself online and my use of ICT will not interfere with my work duties and will always be in accordance with the school AUP and the Law.
6. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.
7. I will promote online safety with the children in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
8. If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the Designated Safeguarding Lead or the Headteacher.
9. I will report any incidents of concern regarding children's online safety to the Designated Safeguarding Lead as soon as possible.
10. I understand that if the school believes inappropriate use or unacceptable behaviour is taking place, the school may invoke its disciplinary procedure. If the school suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation.

Signed:	**Date:**

Appendix 7: Wi-Fi Acceptable Use Policy.

As a professional organisation with responsibility for children's safeguarding it is important that all members of the school community are fully aware of the schools' boundaries and requirements when using the school Wi-Fi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

This is not an exhaustive list and all members of the school community are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

1. The school provides Wi-Fi for the school staff.
2. I am aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. The School takes no responsibility for the security, safety, theft, insurance and ownership of any device used within the School premises that is not the property of the School.
3. The use of ICT devices falls under Harrietsham C of E Primary School's Acceptable Use Policy, online safety policy, Mobile Phone policy and Staff conduct policy, which all staff must agree to and comply with.
4. The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.
5. School owned information systems, including Wi-Fi, must be used lawfully; I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
6. I will take all practical steps necessary to make sure that any equipment connected to the schools' service is adequately secure, such as up-to-date anti-virus software, systems updates.
7. The school's wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school's wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. I confirm that I knowingly assume such risk.
8. The school accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the school's wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.
9. The school accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school's wireless service.
10. I will respect system security; I will not disclose any password or security information that is given to me. To prevent unauthorised access, I will not leave any information system unattended without first logging out or locking my login as appropriate.
11. I will not attempt to bypass any of the schools' security and filtering systems or download any unauthorised software or applications.
12. My use of school Wi-Fi will be safe and responsible and will always be in accordance with the school AUP and the Law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.
13. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.
14. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead as soon as possible.
15. If I have any queries or questions regarding safe behaviour online, I will discuss them with the Designated Safeguarding Lead.
16. I understand that my use of the school Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school may terminate or restrict usage. If the school suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.

Signed:	**Date:**

Appendix 8: PTFA, OPAL and Forest School Social Networking Acceptable Use Policy.

1. As part of the school's drive to encourage safe and appropriate behaviour online, I will support the school's approach to online safety. I am aware that Facebook, Instagram, X are public and global communications tool and any content posted may reflect on the school, its reputation and services.
2. I will not use any School / PTFA badged site to express any personal opinions or create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring the school into disrepute.
3. I will not disclose information, make commitments or engage in activities on behalf of the school without authorisation from the Headteacher.
    - The Headteacher retains the right to remove or approve content posted on behalf of the school.
    - Where it believes unauthorised and/or inappropriate use of the or unacceptable or inappropriate behaviour may be taking place, the school will exercise the right to ask for the content to be deleted or deactivated.
4. I will ensure that any content posted abides by copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.
5. I will follow the school's policy regarding confidentiality and data protection/use of images.
    - I will ensure that the school has written permission from parents/carers before using images or videos which include any members of the school community.
    - Any images of pupils will be taken on school equipment, by the school and in accordance with the school image policy. Images which include pupils will only be uploaded by the school via school owned devices. Images taken for the sole purpose of inclusion will not be forwarded to any other person or organisation.
6. I will promote online safety in the use of Facebook and will help to develop a responsible attitude to safety online and to the content that is accessed or created.
7. I will set up a specific account/profile using a school provided email address to administrate the site and I will use a strong password to secure the account.
    - The school Designated Safeguarding and school Senior Leadership Team will have full admin rights to the account.
8. I will ensure that the content and channel is suitable for the audience and will be sensitive in the tone of language used. I will ensure content is written in accessible plain English.
9. I will report any accidental access or receipt of inappropriate materials or inappropriate comments to the Designated Safeguarding Lead immediately.
10. I will ensure that Facebook is moderated on a regular basis.
11. I have read and understood the school online safety policy which covers the requirements for safe ICT use, including using appropriate devices and the safe use of social media.
    - I have ensured that the site has been suitably risk assessed and this use has been agreed by the Headteacher.
12. If I have any queries or questions regarding safe and acceptable practise online, I will raise them with the Designated Safeguarding Lead.

Signed:	**Date:**

Appendix 9: 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.
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.