The Coombes CE Primary School
Online Safety Policy

Rename – IT Security and Acceptable Usage Policy

Aim of Policy: This policy outlines what The Coombes CofE Primary School will do to ensure the online safety and security of the children in their care. It incorporates the Wokingham 'All in one' V1.3 policy and the advice from the UK Safer Internet Centre website. The Coombes CofE Primary School has personalised this model policy. This is a working document, in order to continually reflect new national guidance and to provide more relevant and specific information about our school's preventative strategies, procedures and sanctions.

For the purposes of this document, the term staff refers to teachers, teaching assistants, governors, office staff, support staff, lunchtime controllers or anyone employed by the school, unless otherwise specified within the document

Description: The policy recognises that at The Coombes CofE Primary School we believe everyone has the right to feel safe, and secure within a caring Christian environment. The Coombes CofE Primary School recognises its responsibilities for safeguarding children and protecting them from harm. All parents/carers are made aware of the school's responsibilities in regard to online safeguarding procedures through publication of the policy on the school's website. Reference will be made to it in the school prospectus and home school agreement. A copy can be obtained from the school by request.

The Coombes Author:	K Foster	**Lead Governor:**	L Connelly
Approval by:	FGB	**Team Reviewing:**	FGB
Based on Model Policy?	Yes	**Date uploaded to website:**	January 2023

Approved by:	FGB	**Date:**	January 2023
		Next Review Date:	January 2024

Contents

1.0 Roles and Responsibilities

1.1 Governors

The Governors are responsible for the approval of the Online Safety Policy (including Acceptable Use Agreements), ensuring that it is implemented and reviewing its effectiveness. In fulfilling this responsibility, the governing body has an appointed Safeguarding governor (who oversees all safeguarding arrangements (including Online safety). The safeguarding governor will undertake the following regular activities:

- Meetings with the member of staff responsible for online safety.
- Monitoring of online safety incident logs.
- Reporting to relevant governor committees.
- Keeping up to date with school online safety matters.

1.2 Headteacher

The Headteacher is responsible for ensuring the overall safety, including online safety, of members of the school community. The Designated Safeguarding Lead (DSL) holds a responsibility for online safety as part of their role (Keeping Children Safe in Education statutory guidance). On a practical day to day basis, others may have particular duties relating to Online Safety, e.g. an Online Safety Co-ordinator, ICT/Computing Subject Leader, Technical support contractors. However, the Headteacher will ensure the following:

- Staff with online safety responsibilities receive suitable and regular training enabling them to carry out their online safety roles and to train other colleagues as necessary.
- The Senior Leadership Team (SLT) / Governing body receives regular monitoring reports e.g. termly safeguarding reports.
- There is a clear procedure to be followed in the event of a serious online safety allegation being made against a member of staff.

1.3 Online Safety Co-ordinator

As noted above, the Designated Safeguarding Lead holds a responsibility for online safety as part of their role (referenced in Keeping Children Safe in Education statutory guidance). The school may opt to appoint an Online Safety Co-ordinator to assist the DSL in their duties. The Online Safety Co-ordinator may in turn work with others (e.g. the ICT/Computing Subject Leader, technical support contractor) to ensure that policies are put into practice. The specific duties of an Online Safety Co-ordinator would need to be confirmed in conjunction with the DSL to ensure absolute clarity about responsibilities, but might include:

- Take a leading role in establishing and reviewing the school's Online Safety Policy and associated documents.
- Provide training and advice for staff and ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provide materials and advice for integrating online safety within schemes of work and check that online safety is taught on a regular basis.
- Liaise with the school's Designated Safeguarding Lead.
- Liaise with the school's IT technical staff.
- Ensure that online safety incidents are reported and logged and used to inform future online safety developments.
- Report to the governors and meet with them as required.
- Agenda item on all SLT meetings / Governing body meetings

1.4 IT Technician/Network Manager/Support Provider

The IT Technician/Network Manager/Support Provider will be responsible for ensuring that all reasonable measures have been taken to protect the school's network(s). This will involve ensuring the following:

- The IT infrastructure is secure and protected from misuse or malicious attack.
- The school meets the online safety technical requirements outlined in any relevant online guidance.
- Users may only access the school's network(s) through a properly enforced password protection policy.
- The school's filtering policy is applied and updated as appropriate.
- Any inappropriate use of the school's computer systems should be reported to the Online Safety Lead/Head Teacher.
- Provide secure external access to the school network as appropriate.

1.5 Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- They are familiar with current online safety matters and the school's Online Safety Policy and practices.
- They have read and understood the school's Staff Acceptable Use Policy (AUP) and signed to indicate agreement.
- They report any suspected misuse or problem to the Online Safety Co-ordinator or DSL for investigation and action.
- Electronic communications with pupils should be on a professional level and only carried out using approved school IT systems.
- Online safety issues are embedded in all aspects of the curriculum and other school activities.
- Pupils understand and follow the school's Online Safety and Acceptable Use Policies.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations in relation to their age.
- They monitor IT activity in lessons, extra-curricular and extended school activities.
- They are aware of online safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement school policies with regard to these devices.
- They know and follow the procedure for dealing with any unsuitable material that is found in internet searches.

1.6 Designated Safeguarding Lead (DSL)

The DSL holds the responsibility for online safety as part of their role (Keeping Children Safe in Education statutory guidance). They should be trained in online safety issues and be aware of child protection matters that may arise from any of the following:

- Sharing or loss of personal data
- Access to illegal/inappropriate materials
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming
- Cyberbullying

1.7 Data Protection Officer (DPO)

The DPO has a related role which is detailed in Data Protection policies and related documentation.

2.0 Reviewing, Reporting and Sanctions

2.1 Review

- This policy will be reviewed and updated annually, or more often if necessary.
- The school will audit provision to establish if the Online Safety Policy is adequate and that its implementation is effective.

2.2 Acceptable Use Agreements

- All users of school IT equipment will sign the appropriate Acceptable Use Agreement. This includes all staff and pupils.
- Parents are asked to sign to show agreement with and support for the school's policy

[See 'Appendix 3 – Exemplar Acceptable Use Agreements' for further information]

2.3 Reporting and logging

- The school will produce clear guidelines as to what should be done if inappropriate content is found when accessing the internet.
- Any such occurrence will be logged for review and any necessary actions that arise.
- All pupils and teachers should be aware of these guidelines.

[See 'Appendix 1]

2.4 Complaints regarding internet use

- Any complaints relating to internet misuse should be made in accordance with the school's existing complaints procedure.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

2.5 Sanctions

- Failure to comply with the requirements of this policy will be dealt in line with the school's existing policies on behaviour, rewards and sanctions.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 or other related legislation. This would constitute a disciplinary matter in the case of staff.

3.0 Communications & Communication Technologies

3.1 Mobile phones and personal handheld devices

- Pupils will not be allowed to bring mobile phones to school unless prior arrangements are made with the school.
- Year 6 pupils who have sought permission, are asked to switch off their phone and hand it in to their class teacher during the school day where it will be stored securely
- The sending of abusive or inappropriate messages or images is forbidden.
- Pupils will not be allowed to bring in games devices, particularly those which allow ad hoc networks to be established.

- Teacher/parent contact should normally be by the main school telephone and not via a mobile device except where off-site activities dictate the use of a mobile phone and with permission from Head Teacher/Online Safety lead.
- Parent helpers in school and staff must ensure that they do not send personal messages, either audio or text, during contact time with pupils. If an exceptional emergency arises they should arrange temporary cover whilst they make a call outside of school.
- Staff and pupils may send educational messages (using the School VLE and communication tools) during lesson times if these are part of the curriculum.
- School should be particularly vigilant where mobile phones may be used with children in Foundation Stage. Staff, helper and visitor mobile devices should be switched off or to silent mode during the times that children are present.
- No device in any school building should contain any content that is inappropriate or illegal.

3.2 E-mail and messaging

- Pupils and staff will be informed that the use of school e-mail or messaging accounts may be monitored.
- Pupils should report any receipt of an offensive e-mail or message on school IT systems.
- Pupils should not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone via an e-mail or message.
- Information of a sensitive nature should only be sent using encrypted e-mail.

3.3 Social networking

For the purpose of this policy social networking is considered to be any digital media or medium that facilitates interaction.

- Staff use of social networking should be compatible with their professional role and show the highest standards of integrity.
- Pupil use of social networking should conform to age restrictions.
- If pupils are reported to school staff for having or using an age inappropriate account, parents/guardians will be informed.

[See *'Appendix 2 – Social Networking Guidance'* for further information]

3.4 Internet usage

- Pupils and staff will be informed that internet access will be monitored
- The school will take all reasonable precautions to ensure that users access only appropriate material. Whilst it is not possible to guarantee that unsuitable material will never appear on a school computer, the school will take appropriate measures to prevent a reoccurrence, including contacting the service provider.
- Users must not create, download, upload, display or access knowingly, sites that contain pornography or other unsuitable material that might be deemed illegal, obscene or offensive.
- Unauthorised users must not attempt to disable, bypass or reconfigure any filtering, virus protection or similar.
- All pupils using the internet, and associated communication technologies, will be made aware of the school's online safety guidelines. These are posted near to the computer systems and are also available as the desktop backgrounds when pupils log in to the school network.
- Pupils will receive guidance in responsible and safe use on a regular basis

3.5 Digital and video images

3.5.1 Parental permission

- School will ensure that, where appropriate, consent is obtained for the taking and use of digital and video images of pupils. Such use could include the school website or social media; display material in and around the school or off site; the school prospectus or other printed promotional material; local/national press.
- Pupils will not be identified by name in any title or commentary accompanying digital or video images that is in the public domain, unless specific parental consent has been obtained.
- Where parental permission has not been obtained, or it is known that a pupil should not be photographed or filmed, every reasonable effort will be made to ensure that a pupil's image is not recorded.
- At whole school events (e.g. Sports day / Christmas play), a common sense approach will be implemented. Parents will be reminded that the taking of any photos is for their private use and no images of any children, other than their own, are to be shared online.

3.5.2 Storage and deletion

- Images should be uploaded to a secure location that is the control of the school. Where memory cards, USB drives, CDs or cloud storage are used during the process of capture or transfer, users should ensure that these are deleted and cleared from any temporary storage or recycle bins.
- Images should be deleted in line with the school's procedures on data retention and disposal.

3.5.3 Recording of images

- School digital devices should always be used to record images of pupils (subject to any variation the school agrees as noted below in 'Use of staff personal devices').
- All pupils appearing in images should be appropriately dressed.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- All digital devices capable of taking photographs and recording sound or video, whether belonging to the school or personal, may be subject to scrutiny if required.
- Where volunteers are supporting school staff, they should abide by the same rules as school staff.

3.5.4 Use of staff personal devices

It is recognised that the most straightforward approach is not to allow use of staff personally owned devices (e.g. staff smartphones, personally owned cameras) to record images. Where school wishes to vary from this, e.g. for off-site activities, the following should apply:

- It will be clearly understood under what circumstances it is permissible to use a personal device. Permission must be sought before use.
- The Head Teacher, DSL and Online Safety Lead have permission from the Governors to take photos on their devices for use on the school website/publicity [See Appendix 3 for further information]
- Images will be transferred to a secure location on the school's system as soon as possible and the originals/any copies fully deleted.
- Such staff personal devices should be passcode protected

3.5.5 Parents taking photographs or video

Where school chooses to allow the recording of images at 'public' events the following should apply:

- Images may only be recorded for personal use and can only be shared with family and friends. They must not be shared on social networking sites or other websites that are accessible by the general public.
- Parents will be reminded at the beginning of any such event that the images are for their private use and no images of any children, other than their own, are to be shared online.

3.5.6 **Events/Activities involving multiple schools**

- When taking part in events organised by other schools or organisations, e.g. sports or music events, it is reasonable to expect that specific image guidelines should be in place and where relevant, include reference to press images.
- Those attending the event will be informed of the image guidelines that apply, e.g. a letter before the event, announcement at the event, or information in any printed programme.
- Although school will make reasonable efforts to safeguard the digital images of pupils, parents should be made aware that at some types of event it is not always realistic to strictly enforce image guidelines. School cannot therefore be held accountable for the use of images taken by parents or members of the public at events.

4.0 Infrastructure and Security

4.1 Security

The Headteacher / Online safety lead will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that procedures outlined within this policy are implemented by those responsible.

- School IT technical staff/IT support contractor may monitor and record the activity of users on the school IT systems and users will be made aware of this.
- Servers, and communications cabinets should be securely located and physical access restricted.
- Wireless systems should be appropriately secured
- All users will have clearly defined access rights to school IT systems.
- Access to the school IT systems will cease when a pupil leaves or, in the case of a member of staff, ceases to be employed by the school.
- Appropriate procedures are in place for secure storage and access to 'Administrator' passwords.

4.2 Passwords

All staff and pupils are provided with an individual password.

- 'Strong' passwords should be used.
- Staff will be asked to change their network password regularly.
- No individual should tell another individual their password.
- No individual should log on using another individual's password, unless they are a member of staff logging on as a pupil for sound educational or technical reasons.
- Once a computer has been used, users must remember to log off.
- Users leaving a computer temporarily should lock the screen (Windows key + L on a PC).

4.3 Filtering

School maintains and supports the managed filtering service provided the Internet Service Provider (ISP).

- Changes to network filtering should be approved by the appropriate person(s).
- Any filtering issues should be reported immediately to the ISP.

4.4 Virus protection

- All computer systems, including staff laptops/devices, are protected by an antivirus product administered centrally and automatically updated.

4.5 Staff laptops/devices and flash drives

Where staff laptops/devices and flash drives are to be taken out of school, it is possible that they may contain sensitive data, therefore school will ensure that all such devices and removable media are password protected.

The following security measures should also be taken with staff laptop/mobile devices:

- USB flash drives with sensitive content data must be encrypted.
- Laptops/devices must be out of view and preferably locked away overnight whether at school or home.
- Laptops/devices should not be used for purposes beyond that associated with the work of the school, e.g. by the family of a member of staff.
- Where others are to use the laptop, they should log on as a separate user without administrator privileges. [See 'Appendix 3 – Acceptable Use Agreements']

4.6 Data protection

See Data Protection Policy for specific guidance in relation to the security of personal data.

4.7 Electronic devices - search and deletion

School has the power to search pupils for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices.

- The Head Teacher/DSL/Online Safety Officer are authorised to examine and/or erase data on electronic devices
- Clear guidance as to what is, and is not, allowed [refer to section 3.1]
- Incidents and outcomes will be recorded using the online safety log

5.0 Online Safety Education

5.1 Learning and teaching for pupils

- Pupils are encouraged to adopt safe and responsible use of IT, the internet and mobile devices both within and outside school through regular online safety lessons and events.
- Pupils are helped to understand the need for an Acceptable Use Policy and, depending on age, asked to sign to indicate agreement.
- Pupils are taught to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Key online safety messages will be included within the curriculum and reinforced as part of a planned programme of assemblies and other appropriate opportunities.
- Rules for the use of computers/devices as well as tips to be safe online are displayed in all rooms and displayed on all pupil desktop backgrounds.

- Incidents with pupils sending inappropriate content intentionally via the internal email message system etc will be dealt with using the schools behaviour policy.

5.2 Staff training

- Staff will be kept up to date through regular online safety training, including National Cyber Security Centre training
- Staff should always act as good role models in their use of IT, the internet and mobile devices.

5.3 Parental support

The support of, and partnership with, parents is encouraged.

- Awareness of the school's policies regarding online safety and internet use; and where appropriate being asked to sign to indicate agreement.
- Advice and guidance on areas (via our school website) such as:
  - filtering systems
  - educational and leisure activities
  - suggestions for safe internet use at home

6.0 Virtual Learning

6.1 Teaching and Learning

- We aim to provide an opportunity for staff and pupils to stay in contact with each other by providing a secure meeting place in which pupils feel less isolated, can talk about things that are important to them and check-in with their classmates and teachers.
- We will use Microsoft Teams VLE, to deliver teaching and learning activities.
- A carefully created a Code of Conduct and User Guidelines are in place to ensure everyone is safe and supported in this Virtual Learning Environment (VLE).
- Staff will provide support pupils in accessing and using the Microsoft Classroom VLE.

6.2 Staff

- Staff will attend appropriate training and will ensure they are confident with online learning tools, updates and staff professional conduct when leading Virtual Learning Sessions
- Staff will model the safe use of technology in the home at all times.
- Positive language and the school behaviour policy will be used at all times.
- Staff will automatically record the learning session for monitoring and safeguarding purposes.

6.3 Parental support

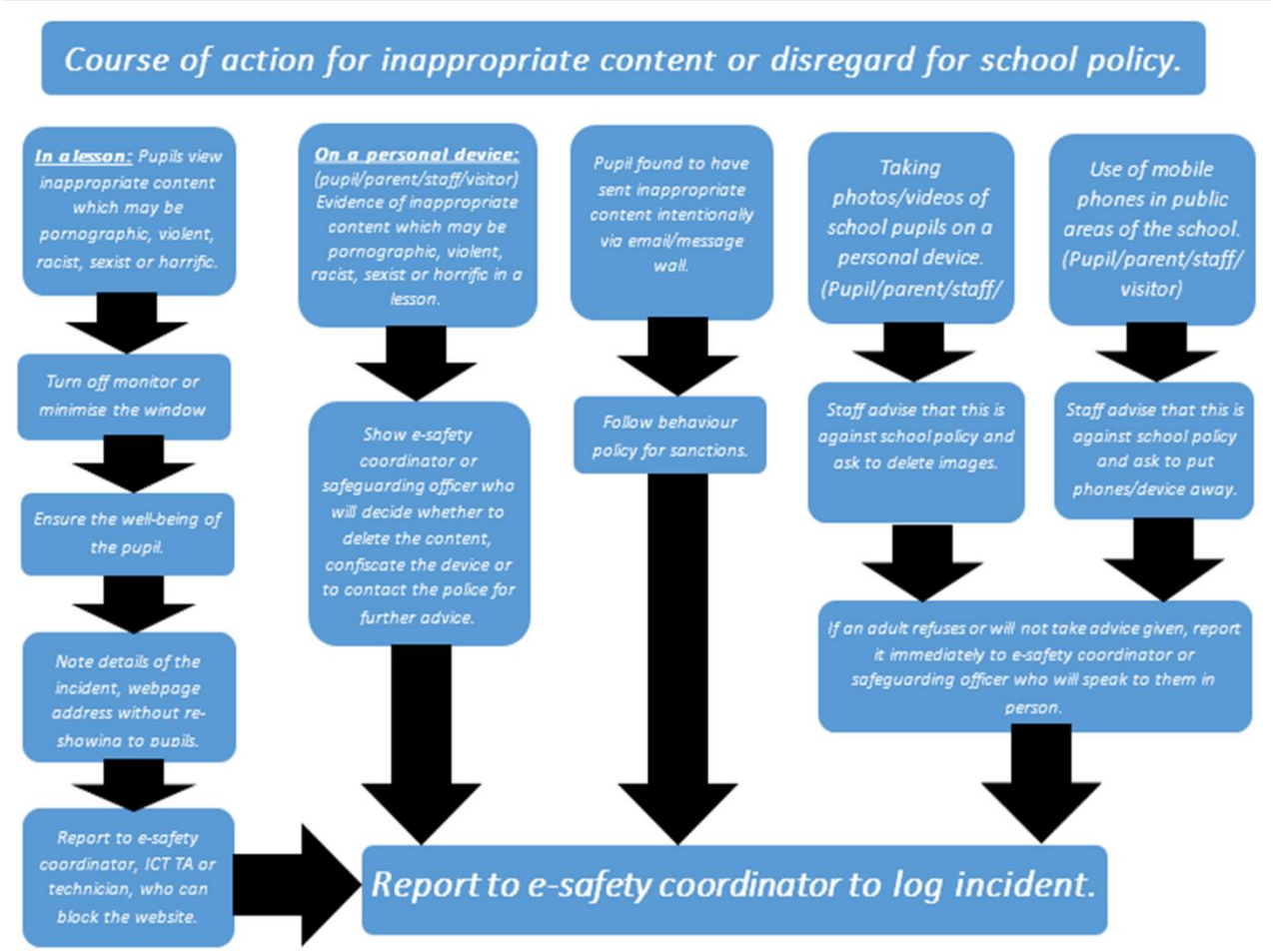
- Parents/carers will be asked to read and sign the Parental Usage Agreement (Appendix 4) to allow school virtual learning sessions to take place
- As the adult in charge at home, parents are expected to reinforce rules for school sessions as well as any other time they are online.
- As children become more confident with using the VLE, parents will need to ensure they monitor how their child is using online resources, particularly as they get older and become more independent.

7.0 Key Personnel

Role	Name	Contact Details
Designated Governor for Online Safety	Louise Connelly	lconnelly@coombes.wokingham.sch.uk
Designated Safeguarding Lead (DSL)	Luke Henderson Kat Foster	head@coombes.wokingham.sch.uk deputyhead@coombes.wokingham.sch.uk
Deputy DSL & Designated Person for Online Safety	Alice Sharman	asharman@coombes.wokingham.sch.uk
Data Protection Officer (DPO)	Jo Hardy	operations@coombes.wokingham.sch.uk
LA Safeguarding Contact/LADO (Local Area Designated Officer)	0118 974 6141	LADO@wokingham.gcsx.gov.uk
Wokingham Safeguarding Children Board (WSCB)	0118 908 8002 01344 786 543 (out of hours duty team)	wscb@wokingham.gov.uk

Appendix 1 – Course of action if inappropriate content is found

- If inappropriate web content is found (i.e. that is pornographic, violent, sexist, racist or extremist) the user should:
  - Turn off the monitor or minimise the window.
  - Report the incident to the teacher or responsible adult.
- The teacher/responsible adult should:
  - Ensure the well-being of the pupil.
  - Note the details of the incident, especially the web page address that was unsuitable (without re-showing the page to the pupils).
  - Report the details of the incident to the Online Safety Co-ordinator.
- The Designated Safeguarding Lead, Online Safety Co-ordinator or other appropriate person will then:
  - Log the incident and take any appropriate action.
  - Where necessary report the incident to the Internet Service Provider (ISP) IT support provider so that additional actions can be taken.



Online Safety - Incident Form
The Coombes Church of England Primary School

Date	
Form completed by	
Nature of incident	
Who was involved: pupils/staff/parents	
Where did it occur	
Time and date incident was logged	
Follow up actions (evidence preserved, senior staff informed, any other action)	
What is in place to prevent a recurrence of this incident?	
Further comments	

Appendix 2 – Social networking guidelines

2.1 Staff conduct

- Staff will always conduct themselves with the highest standards of professional integrity and be aware that how they as individuals are perceived in the virtual world may reflect on how the school is perceived.
- Staff should give careful consideration when posting personal information as to how this might be viewed by pupils and parents, even when the postings are within a 'private' online space.
- Staff should not use the name of the school within their posts/status updates on social networking sites.

2.2 Access to social networking sites

- Social networking sites should never be accessed during timetabled lessons/school working hours
- Staff may not use school equipment to access social networking sites.
- If school chooses to make 'official' use of social networking sites, this should only be by authorised individuals.

2.3 Posting of images and/or video clips

- Photographic images and/or movie clips of children at school or past pupils, up to the age of 18, should never be posted unless specific consent has been obtained from their parent/guardian.
- Photographic images and/or movie clips of school staff should not be posted unless specific consent has been obtained.

2.4 Privacy

- Staff should recognise that their existing lists of friends/contacts/followers may include people who are part of both their private and professional lives.
- Staff should never be online 'friends' with children at the school or past pupils up to the age of 18.
- Staff should not create new links with parents at the school, unless there is a professional reason for doing so. In such instances there should be a clear understanding of the purpose of the link and what 'information' the parent will have access to.
- Profile settings should be regularly checked, and updated as necessary, to ensure that posted comments and images are not publicly accessible.
- Any changes/updates to social networking sites and privacy settings should be clearly understood by the user.

Appendix 3 – Acceptable Use Agreements

3.1 Staff Acceptable Use Agreement *(double sided with laptop/device agreement)*

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. For the purposes of this agreement staff include; teachers, teaching assistants, lunch staff, office staff, governors or anyone else employed in a professional capacity by the school.

I am familiar with the school Online Safety policy (in line with the school code of conduct) and I have read and understand the following:

- IT includes a wide range of systems, including mobile phones, digital cameras, e-mail, social networking and those which are used by or loaned to staff, remain the property of the school and is for the use of Staff members only
- Any equipment provided should be stored and transported securely. Special care must be taken to protect laptops and any removable media devices from loss, theft or damage and take sensible measures to ensure devices are kept in a safe place and not left vulnerable to theft or loss.
- It is a criminal offence to use a school IT system for a purpose not permitted by its owner.
- School information systems may not be used for private purposes and that internet and e-mail may be monitored and recorded to ensure policy compliance.
- The security of the school network will be respected and passwords/security information will only be disclosed to an authorised system manager.
- Software/hardware will not be installed on a school device.
- Personal data, particularly that of pupils, will be stored securely and used appropriately, whether in school, taken off the school premises or accessed remotely in accordance with the school Online Safety policy.
- Copyright and intellectual property rights are to be respected
- Online communication with pupils (within the context of lessons) will be compatible with my professional role.
- Online Safety will be promoted and modelled at all times.
- Pupil internet use, will be consistent with the school's Online Safety Policy.
- Staff know what to do if offensive or inappropriate materials are found on screen or printer and will report any incidents of concern regarding pupils' safety to the appropriate person, e.g. Online Safety Co-ordinator, Designated Safeguarding Lead and/or SLT member.
- Staff will always conduct themselves with the highest standards of professional integrity, be aware that how they as individuals are perceived in the virtual world may reflect on how the school is perceived and give careful consideration when posting personal information as to how this might be viewed by pupils and parents, even when the postings are within a 'private' online space.

The school may exercise its right to monitor the use of the school's information systems, including internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sounds.

Declaration:

I have read and understood the above and also the school's IT Security and Acceptable Usage Policy and agree to abide by the rules and requirements outlined.

Please return this form to the Operation Manager

Name:	
Position:	
Signature:	
Date:	

Personal Device - Acceptable Use Agreement/Permission

The Governors of The Coombes CofE Primary School grant permission for the following named person to use their personal device for school use.

Name	
Position/Role	
Device	
Reason	

I _____ (print name) agree to ensure that the device I use to record and store images/video is password protected/encrypted and will only be used for school use (as directed by the school).

I will not share images with others or to a personal 'cloud' account and I will delete them from my personal device as soon as possible.

Signed	
Dated	

Louise Connelly
Safeguarding & Online Safety Governor

Chair of Governors

3.2 Student/Pupil Acceptable Use Agreement

This agreement will be discussed with pupils during online safety lessons. The wording may be amended for younger pupils.

For my own personal safety:

- I understand that the school will monitor my use of school devices and digital communications.
- I will not tell anyone my username or password nor will I try to use any other person's username and password.
- I will be aware of 'stranger danger', when I am communicating online.
- I will not give out any personal information about myself or anyone else when online.
- I will not arrange to meet people offline that I have communicated with online.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

Respecting everyone's rights to use technology as a resource:

- I understand that the school IT systems are for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to download or upload from or to the internet.
- I will not use the school IT systems for online gaming, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

Acting as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use aggressive or inappropriate language
- I appreciate that others may have different opinions to me
- I will not take or distribute images of anyone without their permission.

Keeping secure and safe when using technology in school:

- I will only use approved e-mail or message accounts on the school system.
- I will not use my personal devices in school.
- I will immediately report any damage or faults involving equipment or software.
- I will not open any attachments to e-mails, unless given permission to do so and I know and trust the person/organisation that sent the e-mail.
- I will ask for permission before sending an e-mail to an external person/organisation
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will immediately tell a staff member if I feel uncomfortable about anything I see online

Using the internet for research or recreation:

- When I am using the internet to find information, I should take care to check that the information that I access is accurate.
- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos).

Taking responsibility for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (e.g. cyberbullying, inappropriate use of images and/or personal information).
- I understand that if I break these rules I will be subject to disciplinary action as outlined in the school's Behaviour Policy. This may also include loss of access to the school network/internet.

I have read and understood the above and agree to follow the rules outlined.

Name:	
Signature:	
Date:	

3.4 Parent/Carer Acceptable Use Agreement

In a time where technology is continually evolving, we take Online Safety very seriously at The Coombes CE School and ask parents/carers for their support in this matter. The school expects *students/pupils* to be responsible and safe users of IT.

- As the parent/carer of the above *student/pupil*, I understand that my son/daughter will have access to the internet and to IT systems at school.

- I know that my son/daughter has signed an Acceptable Use Agreement and will receive online safety education to help them understand the importance of safe use of IT – both in and out of school.

- 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 IT systems. I also understand that although internet filtering systems usually work very well, inappropriate content may occasionally still be accessible, but in this instance the school will take appropriate action with the service provider to request such content is removed.

- I understand that my son's/daughter's activity on the IT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety so that home/school can work together.

- I understand that parents/carers are asked not to request staff members as 'friends' on social networking sites.

- I understand that although the school recognises that parents wish to share their children's achievements, posting photos of school pupils on social media sites is potentially sharing them with a much wider audience than intended - without the consent of all those involved. At whole school events (e.g. Sports day / Christmas play), a common sense approach will be implemented. Parents will be reminded that any photos taken, should not to be shared online.

- I understand that parents/carers who volunteer their time in school/school trips, must switch off their mobile phones and not make any calls/messages or take photographs in this time.

Appendix 4 – Acceptable Use During Virtual Learning

4.1 Parent Acceptable Use Agreement - Virtual Learning

As a parent/carer I will:

1. Keep my child's access details to Microsoft Teams confidential.
2. Give 24 hr notice before the lesson should I need to request a login to be reset.
3. Ensure that my child is working in a communal area of the home.
4. Ensure my child is dressed appropriately.
5. Ensure my child follows the school's behaviour policy during learning sessions.
6. Ensure that the webcam and microphone is switched on.
7. Not record video calls.
8. Not engage in conversation with the teacher during the session (questions can be emailed at a separate time).
9. Ensure my child is on time and ready to learn for the beginning of the session.
10. Ensure that my child will complete all tasks to the best of their ability and work is uploaded in the manner required.

I understand that the school will record my child during the virtual learning session, for safeguarding and monitoring purposes.

Name of pupil:	
Parent Signature:	
Relationship to pupil:	

4.2 Pupil Acceptable Use Agreement - Virtual Learning

As a Pupil of The Coombes CofE Primary School, I will:

1. Remember not to share my login or password details.
2. Arrive promptly for the virtual lesson, ready to be admitted to the virtual classroom.
3. Be prepared for the lesson and have all resources ready.
4. Ensure my camera is turned on ready for the session.
5. Ensure my microphone is turned off, unless asked to switch it on by my teacher.
6. Ensure that my learning takes place in a quiet shared family space (not my bedroom)
7. Dress appropriately for my lesson – uniform not necessary.
8. I will not record or share any part of the lessons
9. During the virtual lessons, I will behave as I would in school.
10. I will not use a virtual background.
11. If I wish to speak to the teacher, I will use the *Raised Hand* function.
12. I will complete all given tasks to the best of my ability and hand them in as requested

Name of pupil:	
Class:	