Coupe Green Primary School
HOGHTON

ONLINE SAFETY POLICY
(Including the Acceptable Use Policy)

Our online safety vision statement;

"To equip children with the skills and knowledge they need to use technology safely and responsibly at the school, in the home and beyond."

Online Policy

Online encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing such as online 'blogs' and online forums including Twitter and Facebook. It highlights the need to educate staff and pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

Coupe Green's Online Safety policy operates in conjunction with other policies including those for Child Protection, Behaviour, Anti-Bullying, Curriculum, Relationships and Sex Education, Data Protection, Security and Remote Learning.

Good Practice Regarding Online Safety

Online Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of Online Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from Network Connect including the effective management of Lightspeed FortiGuard web filtering.
- National Education Network standards and specifications.

Introduction

Writing and Reviewing the Online Safety Policy

The Online Safety Policy is part of the School Development Plan and relates to other policies including those for all curricular subjects, behaviour, anti-bullying, cyber bullying and child protection.

- Coupe Green's Online Safety co-ordinator is the Computing Coordinator, however on-line safety is also monitored by our Headteacher, ensuring that all safeguarding measures are effective.
- Our Online Safety Policy has been written by the school, building on the Lancashire Online Safety Policy and government guidance. It has been agreed by senior management including EYFS leader, and approved by governors

- The Online Safety Policy and its implementation will be reviewed annually.
- The Online Safety Policy was revised by the Senior Leadership Team and the Online Safety Champion.
- It was approved by the Governors in May 2021.

The School's Online Safety Champion

The Online Safety Champion is the main point of contact for Online Safety related issues and incidents. The role of the Online Safety Champion includes:

- Having operational responsibility for ensuring the development, maintenance and review of the school's Online Safety Policy and associated documents, including Acceptable Use Policies.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an Online Safety incident occur.
- Ensuring an Online Safety Incident Log is appropriately maintained and regularly reviewed. APPENDIX 8 – Online Safety Incident Log
- Keeping personally up-to-date with Online Safety issues and guidance through liaison with the Local Authority and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Providing or arranging Online Safety advice/training for staff, parents/carers and governors.
- Ensuring the Head, SLT, staff, children and governors are updated as necessary.
- Liaising closely with the school's Designated Safeguarding Lead (DSL) to ensure a coordinated approach across relevant safeguarding areas.

Some of the above responsibilities may be delegated to appropriate members of staff.

Security and Data Management

ICT security is a complex subject that involves all technology users in the school, dealing with issues regarding the collection and storage of data through to the physical security of equipment. The Lancashire ICT Security Framework (published 2005) should be consulted to ensure that procedures are in place to ensure data, in its many forms, is kept secure within the school.

In line with the requirements of the General Data Protection Regulation (GDPR 2018) sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be:

1. **Accurate**
2. **Secure**
3. **Fairly and lawfully processed**
4. **Processed for limited purposes**
5. **Processed in accordance with the data subject's rights**
6. **Adequate, relevant and not excessive**
7. **Kept no longer than is necessary**
8. **Only transferred to others with adequate protection.**

All data in school must be kept secure and staff informed of what they can or can't do with data through the Online Safety Policy and statements in the Acceptable Use Policy APPENDIX 2 – ICT Acceptable Use Policy (AUP) – Staff and Governor Agreement

APPENDIX 3 - ICT Acceptable Use Policy (AUP) – Supply Teachers and Visitors/Guests Agreement

Supply Teachers only have access to the public drive so lesson presentations must be saved in their supply teachers folder. Always use the supply teacher login for supply teachers.

Curriculum data is backed up in school, and Admin data is backed up remotely by TechHub.

Staff are permitted to use pen drives and other similar devices to transfer none personal information such as lesson plans and resources for use in school and at home. All pen drives are encrypted to ensure that data is safe.

Assessment data, such as 'Foundation Trackers', are stored on the Teacher's Shared Drive on the school network, access to which is restricted by password to staff only. Staff are instructed not to store electronic copies of this data at home.

The data for core subjects is stored on the Lancashire Tracker and again can only be accessed with an allocated login and password.

There is currently no remote access to school network from home, however during school closures School Business Managers and School Business Support Staff have been granted access to the school network from home to ensure that systems continue to run effectively.

School does allow the use of 'cloud' storage facilities e.g. One drive for external storage that is none confidential data. All personal data is password protected within the One drive system.

We have one wireless network (Coupe Green wireless) in school, and it is password protected and secure.

The Use of Mobile Devices

School use of mobile devices, including laptops, tablets, mobile phones, cameras and games consoles is becoming more commonplace. Whilst these can provide a flexible solution and offer a range of exciting opportunities to extend children's learning, their use poses challenges in terms of online safety. Many of these devices integrate functionality to take images, access the Internet and engage users in various methods of external communication.

Mobile Phones

Mobile phones can present a variety of challenges if not used appropriately. Smart phones can upload pictures onto cloud storage so even if you delete picture from phones memory, it's still stored on cloud. They are valuable items that can be lost, stolen or damaged in the school environment and could also be considered as distracting or intrusive in a teaching or learning situation. However, staff and parents may equally have valid reasons why mobile phones should be readily available.

In order to balance the benefits of mobile phones alongside the possible issues they can create, the school has a number of guidelines in place:

- Staff are permitted to use mobile phones in school before the start of the school day, during break times, at lunch and after the school day has ended as long as this use is away from the children (i.e. staffroom or office)
- Children are not permitted to have mobile phones in school
- In the event of a child bringing a mobile phone into school the phone is removed and stored in the office and the parents contacted to remind them of the school rules regarding mobile phones.
- Parents are asked not to use mobile phones inside the school premises or outside when a lesson is taking place. A notice is on display to remind visitors of the rule.
- Staff are responsible for the security of their own belongings, including mobile phones, and, on request, can store them securely in the school office.
- Staff are advised that it is good practice to store their mobile phones in 'silent' mode or off during lessons to reduce the risk of disturbance or inconvenience to others. All staff mobiles should be stored safely and away from sight of pupils.
- Images of children video or audio must not be recorded on personal mobile phones.
- Where it is essential for a staff member to leave their phone on to receive an emergency call, this must have been agreed and discussed with a member of the SLT

Child Protection policy page 10 "USE OF MOBILE PHONES AND CAMERAS"

- The school office can always be contacted in the event of an emergency.
- Lunchtime supervisors leave their phones off or in designated areas.
- **Warning!** Mobile phones have access to the Internet; this is NOT filtered and could lead to unsuitable content being viewed.
- Any suspicious use of mobile phones and / or cameras, report to the Headteacher.

The Misuse of Mobile Phones

Mobile phones are one potential source of cyber bullying. The issue of cyber bullying is discussed with the children as part of the online safety/RSE curriculum. The school reserves the right to confiscate a phone or device if there is good reason to believe that it is being used to contravene the school's behaviour policy. In the event of such action being required the head teacher or a member of the SLT would be informed and involved in the process and parents would be informed of the reasons for the action.
Staff are asked to be vigilant in monitoring visitors for any covert use of mobile phones or cameras and to report any concerns to the head teacher.

Other Mobile Devices

The rules for mobile phone use in school apply to all other mobile devices.

- When permission to use such devices is granted it is expected that the relevant security settings, such as passwords and anti-viral protection, are in place and up to date.
- The owners of the devices are responsible for ensuring that all the content held on them is legal and should understand that the school cannot be held liable e.g. for any damage or theft of personal devices.
- Such devices can only be used on the school's network, e.g. to transfer data by Blue-Tooth or to access the Internet using Wi-Fi, after obtaining the express permission of the head teacher and should be checked first to ensure that they contain no viruses or mal-ware that may cause damage to the school's systems.
- As with mobile phones, inappropriate use of such devices may lead to their confiscation.

Use of Digital Media

(Cameras and Recording Devices)

The use of cameras and sound recording devices offer substantial benefits to education but equally present schools with challenges particularly regarding publishing or sharing media on the Internet, e.g. on Social Network sites.

Photographs and videos of children and adults may be considered as personal data in terms of GDPR (2018).

Consent and Purpose

- Written consent is collected from parents for photographs of their children to be taken or used. Permission is given through a general written consent form issued to all families (Appendix 5 to 7)
- Staff are informed of any children whose parents or guardians have not given their consent for their photographs to be taken or their images used in digital form by the school. A list is compiled by the school office and is updated when consent forms are reissued. It is the responsibility of staff to ensure that only images containing children whose parents or guardians have given permission are used by the school. Verbal consent is not considered acceptable.
- Images of staff or adults employed in the school will not be used without their written consent. A consent register for use of images will be stored in the school office.
- It is made very clear, when gaining consent, how photographs can / cannot be used (including the use of external photographers or involvement of 3rd parties).
- Written consent includes permission to store / use images once a child has left the school e.g. for brochures, displays etc… Parents should be informed of the timescale for which images will be retained.
- Written permission forms will be issued to parents. In the event of any circumstances that may necessitate removal of permission the list of children will be amended and reissued to all staff concerned.
- Parents are informed of the purposes for which images may be taken and used e.g. displays, website, brochures, press and other external media.
- Images that at times may be displayed in public areas, e.g. the entrance hall, are subject to the same restrictions.
- Parental permission is required for their child's images to be included in portfolios maintained by trainees and students not directly employed by the school.
- Parental permission is required to use group images in individual children's profiles e.g. an image of a group activity in EYFS that is included in several children's profiles.
- Images are not used of children or adults who have left the school unless their written permission has been obtained.
- Written permission from parents is required when children's images are used by the press. Permission is required if the press wish to name individual children to accompany a photograph or if the media publish an image in their online publication which may offer facilities for the 'public' to add comments in relation to a story or image and can potentially invite negative as well as positive comments.

Taking Photographs / Video

- Evidence Me is used across the whole school; therefore, consent has been given directly for this. Parents have responded to an email and agreed to this separately. Photographs are sent to parents via this software.

- Teachers and Teaching Assistants are authorised to take images related to the curriculum. Other adults taking photographs must be designated by the Headteacher.
- Photographs and videos are only taken using **school owned equipment**, including memory cards, digital tape and disks. The use of personal equipment to store images is not permitted.
- When taking photographs and video the rights of an individual to refuse to be photographed are respected.
- Photographs must never show children who are distressed, injured or in a context that could be embarrassing or misinterpreted.
- Care is taken to ensure that individual children are not continually favoured when taking images.
- The subject of any film or photograph must be appropriately dressed and not participating in activities that could be misinterpreted e.g., particular care may be needed with the angle of shots for children engaged in PE activities.
- Certain locations are considered 'off limits' for taking photographs, e.g. toilets, cubicles, etc…
- Discretion must be applied with the use of close up shots as these may be considered intrusive. Shots should preferably include a background context and show children in group situations.

Parents Taking Photographs / Videos

Under the General Data Protection Regulation 2018, parents are entitled to take photographs of **their own** children on the provision that the images are for **their own** use, e.g. at a school production. Including other children or other purpose could constitute a potential breach of Data Protection legislation.

- Parents are informed that they should only take photographs of their own children and that they need permission to include any other children / adults.
- Parents are reminded that publishing images which include children other than their own or other adults on Social Network sites is not acceptable, unless specific permission has been obtained from the subjects and, in the case of children, their parents.

Storage of Photographs / Video

- Photographs are securely stored and should not be removed from the school environment unless for a specific purpose and with the head teacher's consent. In this instance the data must be kept secure and must be erased after use. This could include storage of images on portable devices e.g. laptops or tablets.
- Images should be stored on tablets for the minimal amount of time. Only images intended for a specific purpose should be stored. They must be stored securely and be deleted once they have been used
- IPads are networked so that images can be saved onto the Teacher's Drive.
- Staff should not store images on personal equipment e.g. tablets, laptops or USB storage devices.
- Staff should not store personal images on school equipment unless they have a clear purpose e.g. to support in the teaching of a lesson. Once used, the images should be deleted.
- Access to photographs / videos stored on school's equipment is restricted to school staff. The server allows data to be stored so that it accessible either to all staff, teachers or pupils.
- Individual members of staff are responsible for deleting photographs / video or disposing of printed copies (e.g. through confidential waste systems) once the purpose

for the image has lapsed. The ICT Co-ordinator and IT manager have access to all areas of the network and can assist with the removal of data.

- Should a parent withdraw permission the class teacher is responsible for the removal and deletion of images and may be assisted by the ICT coordinator.
- Photographs sent electronically must be sent securely. This is done using staff accounts on the Lancashire e-mail system. Private email is not accessed in school using the school's equipment.

Publication of Photographs / Videos

- Consent is needed from parents for publication of children's images, e.g. on a website.
- Photographs should only be published online to secure sites.
- When publishing photographs, care should be taken over the choice of images to ensure that individual children / adults cannot be identified or their image made available for downloading or misuse, e.g. through the use of low definition images that will not magnify effectively, eg using Image Resizer in Windows or the flash upload app on the school website.
- Full names and / or other personal information should not accompany published images.
- If very high quality pictures are uploaded they are put in a password protected part of the school website, the password is sent home in the newsletter but removed on the web version of the newsletter.

When Publishing Images

- Children's images taken in school should not be displayed on insecure sites e.g. personal social networking sites. Parents and staff are informed in writing of this. If such images are reported their immediate removal will be requested.
- Staff and children are made aware that full names and personal details will not be used on any digital media, particularly in association with photographs.
- All staff should recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites. Staff should ensure that personal profiles are secured and do not display content that is detrimental to their own professional status or could bring the school into disrepute.

The Media, 3rd Parties and Copyright

- Visiting third parties within school are supervised at all times whilst in the school and are expected to comply with the Data Protection requirements in terms of taking, storage and transfer of images.
- The copyright for images taken by a 3rd party must be made clear beforehand and agreed by the school and parents before such images are used, eg in a local newspaper.
- If uploading images to a 3rd party website, e.g. for printing or creating calendars, cards etc, staff are expected to read and be familiar with read the terms and conditions of the web site. (You could unknowingly be granting the site's host licence to modify copy or redistribute your images without further consent. The site may also be advertised for 'personal use' only – therefore using for business purposes would be a breach of the terms and conditions).

CCTV, Video Conferencing, VOIP and Webcams

- Parents should be informed if CCTV, video conferencing or webcams are being used in the school.

- Parents are required to give written permission for their child/children to participate in activities that include taking of video and photographs. Although children may not be appearing 'live' on the Internet through a video conferencing link, it is still important to remember that the images which are broadcast from school could be captured as a snapshot or video clip from a system receiving the broadcast.
- Video conferencing (or similar) sessions should be logged including the date, time and the name of the external organisation/ person(s) taking part.
- The purpose for using CCTV /video conferencing or webcams should be made clear to those liable to be included in footage taken by these resources.
- When used cameras should not overlook sensitive areas, e.g. changing rooms or toilets.
- The headteacher would have overall access to any recordings made and would supervise their secure storage and deletion.
- Consideration is required regarding copyright, privacy and Intellectual Property Rights (IPR) legislation.
- Recordings are not repurposed in any other form or media other than the purpose originally agreed.
- Image Consent forms can be found in the Appendices (5 to 7).

Communication Technologies

School uses a variety of communication technologies, each of which carries various benefits and associated risks. All new technologies should be risk assessed against the potential benefits to learning and teaching before being employed throughout the school. Ideally this should be done before multiple devices are purchased. As new technologies are introduced, the Online Safety Policy will be updated and all users made aware of the changes. The policy is reviewed annually.

Email

- The Lancashire Office 365 service is the preferred school email system.
- Staff should not access personal email accounts during school hours on school equipment unless prior permission is obtained from the head teacher and access is required for professional purposes.
- E-mail accounts for children are organised as class accounts or computer, eg Year4. This ensures that children cannot be identified through an individual e-mail address.
- Only official email addresses should be used to contact staff or children.
- Office 365 Learning filtering service is employed to reduce the amount of SPAM (Junk Mail) received on school email accounts. BT Lancashire Services get all the email entered into the school SPAM filter and reports to ‘BT One Connect’.
- All users should be aware of the risks of accessing content including SPAM, phishing, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail. Notices put in staffroom of new SPAM outbreaks.
- All users should be aware that email is covered by GDPR (2018) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.
- All users should also be aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.
- Staff are responsible for monitoring the content of children’s email communications, both outgoing and incoming messages.
- Users must report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. Children are taught how to respond in such situations

by reporting immediately to the adult in charge at that time. Staff report to senior leaders within the school and can report to Lancashire directly.

- Users should be aware that they should not open attachments that they suspect may contain illegal content as they could inadvertently be committing a criminal act.
- All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
- We always tell an adult if we see anything we are uncomfortable with. APPENDIX 7 – Typical Classroom Online Safety Rules (KS2)
- We always tell a trusted adult if we find something that upsets us. APPENDIX 6 – Typical Classroom Online Safety Rules (EYFS KS1)

Social Networks

Social Network sites allow users to be part of a virtual community. They include sites such as Facebook, Twitter, Instagram and TikTok. These sites provide users with simple tools to create a profile or page including basic information about themselves, photographs, and possibly a blog or comments. As a user on a Social Network site, it may be necessary to access and view other users' content, send messages and leave unmediated comments. Many Social Network sites are blocked by default through filtering systems used in schools, but these settings can be changed at the discretion of the headteacher (See http://N.lancsngfl.ac.uk/lgfladvice/index.php for more details).

Where social networking sites are used, staff should always conduct themselves in a professional manner. If content is made available on the web it is available for everyone to see and potentially remains there forever.

Facebook is only enabled on the headteacher's computer, which does not allow free access to anyone else in school. School Facebook posts are therefore monitored by the headteacher.

All staff need to be aware of the following points:

- The content on Social Network sites may be unmediated and inappropriate for certain audiences.
- If a Social Network site is used personally, details must not be shared with children and privacy settings be reviewed regularly to ensure information is not shared automatically with a wider audience than intended.
- Staff must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.
- Any content posted online should not bring the school into disrepute or lead to valid parental complaints. It should not be deemed as derogatory towards the school and/or its employees or towards pupils and/or parents and carers. It should not bring into question the appropriateness of staff to work with children and young people.
- Adults must not communicate with children using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted. Online Communications with parents, past pupils or siblings of pupils, especially if under the age of 18 should be discouraged.
- Children must not be added as 'friends' on any Social Network site. School's advice to parents in relation to their use of Social Networking Sites and how the school will respond to identified issues is to refrain from posting inappropriate comments about staff or children that could be construed as instances of cyber bullying. Parents are also requested to refrain from posting images of children or

adults on profiles without permission of the individuals involved, especially if the photographs contain children other than their own.

Instant Messaging or VOIP

Instant Messaging systems, e.g. Text messaging, Skype, Zoom, Facetime, are popular communication tools with both adults and children. They can provide an opportunity to communicate in 'real time' using text, sound and video. The Lancashire Grid for Learning filtering service 'blocks' some of these sites by default, but access permissions can be changed at the request of the headteacher

(See http://www.lancsngfl.ac.uk/lgfladvice/index.php for more details).

Facetime Messenger is disabled on school IPads.

- Staff and children need to be aware of the risks involved using this technology e.g. viewing inappropriate images or making unsuitable contacts.
- Staff do not use school equipment to communicate with personal contacts.
- Only secure messaging, forum or chat systems are used.
- Any communication, e.g text messaging to contact parents, is to be kept secure and contact lists are stored securely in the school office.
- Virtual Learning Environment (VLE) / Learning Platform
- Various systems are being used regularly in schools as communication tools.
- Old accounts on Google Apps and school network are deleted when staff and children leave the school.

Websites and other Online Publications

This may include for example: school websites, Social Network profiles, podcasts, videos, wikis and blogs.

Information posted online is readily available for anyone to see and thus form an opinion about the school. From September 2012, the School Information (England) (Amendment) Regulations 2012 specified that certain up to date information must be made available on a school's website.

More details regarding these requirements can be found on the DfE website or at http://www.legislation.gov.uk/uksi/2012/1124/made
The school website is used as one method to communicate Online Safety messages to parents/carers via links to Online Safety sites and access to the Online Safety policy.

- Everybody in the school who is involved in editing and contributing to the website and is made aware of the guidance for the use of digital media.
- Everybody in the school should also be aware of the guidance regarding the inclusion of personal information on the website.
- Editing online publications is restricted to staff who have the responsibility to ensure that the content is relevant and current.
- Overall responsibility for what appears on the website lies with the headteacher.
- Consideration is given to the use of any content subject to copyright/personal intellectual property restrictions.
- Some content is occasionally hidden behind a password protected area e.g. links to governors information.
- Downloadable materials in a read-only format (e.g. PDF) where necessary, to prevent content being manipulated and potentially re distributed without the school's consent.

- YouTube is used for teaching if the page has already been checked beforehand.
- Pupils are not allowed to use YouTube themselves.
- Pupils are not allowed to use Facebook
- Web site photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

Infrastructure and Technology

School ensures that the infrastructure/network is as safe and secure as possible. Our school's internet and filtering systems are provided by Network Connect, who use Education Connect to provide a managed internet service with full compliance to the DfE online safety requirements.

It is important to note that the filtering service offers a high level of protection but occasionally unsuitable content may get past the filter service. If inappropriate content is viewed or searched in school, Network Connect contact school to inform them along with providing a weekly security report. Sophos Anti-Virus software is included in the school's subscription and is installed on computers and configured to receive regular updates.

Children's Access

- Children are always supervised when accessing school equipment and online materials (e.g. working with a trusted adult). Use of the computers at break and during lunchtimes is prohibited unless in a supervised club.
- Children's access to the school systems by class logins, Individual logins and age appropriate passwords.
- Children's access is restricted to certain areas of the network and computer.

Adult Access

- Access to school systems is restricted for all staff according to their areas of responsibility.

Passwords

- All staff should be aware of the guidelines in the Lancashire ICT Security Framework for Schools. This is available at http://www.lancsngfl.ac.uk/onlinesafety/ website.
- All adult users of the school network have a secure username and password.
- The administrator password for the school network are only available to TechHub Northwest Ltd.
- Staff and children are reminded of the importance of keeping passwords secure.
- Password changes can be requested by staff themselves and also in consultation with the IT Technician.
- Passwords for classes follow name and number
- Passwords for children are made up by the children and they are taught to keep them secret.
- Bug Club and TT Rock Stars passwords are kept secret and children are taught to not share them.

Software/Hardware

- School has legal ownership of all software (including apps on tablet devices).
- School keeps an up to date record of appropriate licenses for all software. This is maintained by the IT Technician who liaises with the School Business Manager.
- An annual audit of equipment and software is made.
- The IT Technician in discussion with the Computing Coordinator and headteacher control what software is installed on school systems.
  Managing the network and technical support
- Any servers, wireless systems and cabling are securely located and physical access is restricted.
- All wireless devices have been security enabled.
- All wireless devices are accessible only through a secure password.
- Relevant access settings should be restricted on tablet devices e.g. downloading of apps and purchases.
- Internet is provided by Network Connect, with Fortinet filters and provides security for internet access. No external access to the school network.
- School systems are kept up to date regularly in terms of security e.g. computers are regularly updated with critical software updates/patches and Sophos antivirus software is automatically updated.
- Users (staff, children, guests) have clearly defined access rights to the school network e.g. They have a username and password and, where appropriate, permissions are assigned.
- Staff and children are reminded to lock or log out of a school system when a computer/digital device is left unattended.
- Users are not allowed to download executable files or install software. The Computing Co-ordinator and IT Manager possess administrator rights and are responsible for assessing and installing new software.
- Users can report any suspicion or evidence of a breach of security to the Computing Co-ordinator, IT Manager or the headteacher.
- School equipment, such as teacher's laptops or cameras, should not be used for personal/family use.
- Any network monitoring takes place in accordance with the Data Protection Act (1998). Staff are told that the network may be monitored from time to time.
- The IT Manager has been provided with a copy of this policy and is aware of the standards required to maintain Online Safety in the school.

Filtering and Virus Protection

- Coupe Green uses Lightspeed Filtering through Fortinet Filtering systems.
- **Prevent Duty**, Light speed is complying with the Government's current Prevent Duty guidance.
- The filtering is managed by the IT Technician, Network Connect, alongside the Computing Coordinator on a monthly basis.
- A weekly report is received by the Headteacher and any concerns investigated.
- SLT members have access to information regarding devolved filtering in school.

- Information regarding devolved filtering is communicated to members of staff through staff meetings and via email. Staff wishing to block or unblock websites may do so by making a request to the IT Manager (Tech-Hub) or Computing Co-ordinator.
- The ICT Manager ensures that all equipment, such as school laptops, used at home are regularly updated with the most recent version of virus protection used in school
- Staff report any suspected or actual computer virus infection to the IT Manager or Computing Co-ordinator.

Dealing with Incidents

An incident log (see Appendix 8) is completed to record and monitor offences. This is audited on a regular basis by the Computing Coordinator and Headteacher.

Any suspected illegal material or activity must be brought to the immediate attention of the headteacher who must refer this to external authorities, e.g. Police, CEOP,s or the Internet Watch Foundation (IWF). Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident.

Always report potential illegal content to the Internet Watch Foundation (http://www.iwf.org.uk). They are licensed to investigate – schools are not! Examples of illegal offences are:

- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred

See chart APPENDIX 9 – Responding to Online Safety Incident Escalation Procedures

Inappropriate Use

It is more likely that school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and actions are proportionate to the offence.

Incident Procedure and Sanctions

APPENDIX 9 – Responding to Online Safety Incident Escalation Procedures.
In the event of accidental access to inappropriate materials; Minimise the webpage/turn the monitor off. Tell a trusted adult.

- Inform the Computing Coordinator, where a log of the incident will be recorded and acted on in line with procedures stated within the policy.

If other people's logins and passwords are used maliciously, inappropriate materials are searched for deliberately, inappropriate electronic files are brought from home or chat forums are used in an inappropriate manner;

- Inform the designated Online Safety Champion
- Enter the details in the Incident Log.
- Implement additional Online Safety training with the individual child or class.
- Take appropriate action in relation to the disciplinary policy, e.g. contact parents.

Acceptable Use Policy (AUP)

The Acceptable Use Policy is intended to ensure that all users of technology within school are responsible and are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes.

The AUP is provided for Staff, Children and Visitors/Guests and must be signed and adhered to by users before access to technology is allowed. The parental agreement is a partnership between parents/carers, children and the school to ensure that users are kept safe when using technology. A list of children who, for whatever reason, are not allowed to access technology will be kept in school and made available to all staff.

The AUP reflects the content of the school's wider Online Safety Policy and is regularly reviewed and updated. It is regularly communicated to all users and is understood by each individual user and relevant to their setting and role/ responsibilities.

(see Appendix 1 to 5)

Education and Training

We recognise that education and training are essential components of effective Online Safety provision. Equipping individuals, particularly pupils, with the appropriate skills and abilities to recognise the risks and how to deal with them is fundamental. Online Safety guidance must be embedded with the curriculum and advantage taken of new opportunities to promote Online Safety. Online Safety messages are communicated to the various stakeholder groups in our school community via Online Safety rules posted in all rooms where computers are used and discussed with pupils regularly.

Online Safety is embedded within the Computing and PSHE scheme of work, in our assemblies and throughout the curriculum. There are three main areas of Online Safety risk that our school is aware of and considers:

AREA OF RISK	**EXAMPLES OF RISK**
Commerce: Pupils need to be taught to identify potential risks when using commercial sites	Advertising e.g. SPAM Privacy of information (data protection, identity fraud, scams, phishing) Invasive software e.g. virus', Trojans, Spyware Premium rate services Online gambling
Content: Pupils need to be taught that not all content is appropriate or from a reliable source	Illegal materials Inaccurate/bias materials Inappropriate materials Copyright and plagiarism User-generated content e.g. YouTube, Flickr, Cybertatto, sexting
Contact: Pupils need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.	Grooming Cyberbullying Contact inappropriate e-mails/instant messaging/blogging Encouraging inappropriate contact

Online Safety- Across the curriculum

It is vital that children are taught how to stay safe, protect themselves from harm and take a responsible approach to their own and others' e-safety. Coupe Green provides relevant, flexible and engaging Online Safety education to all children as part of their curriculum entitlement.

- Regular, planned Online Safety teaching takes place within a range of curriculum areas including Computing and PSHE lessons.
- Teachers consider how Online Safety education can be differentiated for children with special educational needs.
- Coupe Green takes part in the annual 'Safer Internet Day' activities that focus on Online Safety during the National Online Safety Awareness Week.
- During lessons where the internet is used children are made aware of the relevant legislation when using the Internet e.g. GDPR and copyright implications.
- As part of the Online Safety training children are made aware of the impact of cyberbullying and how to seek help if they are affected by these issues, e.g. talking to a trusted adult in school or parent/carer.
- Children are taught to critically evaluate materials and develop good research skills through cross curricular teaching and discussions.
- As part of their Online Safety training and PSHE children develop an understanding of the importance of the Acceptable Use Policy and are encouraged to adopt safe and responsible use of ICT both within and outside school.
- Children are reminded of safe Internet use through corridor and classroom displays and the Online Safety rules that are displayed throughout school in infant and junior classrooms. (See Appendix 6 & 7).

Online Safety– Raising staff awareness

- Online Safety is regularly discussed at staff meetings and during Inset time.
- Courses are available from Lancashire to train staff with overall responsibility for e-safety, e.g. the Computing Co-ordinator and Online Safety champion.
- Online Safety training can be provided in school or from external agencies such as Lancashire advisory service and the police. (CEOP)
- Online Safety training/discussions ensure staff are made aware of issues which may affect their own personal safeguarding e.g. use of Social Network sites.
- All staff are expected to promote and model responsible use of ICT and digital resources.
- Online Safety training is provided within an induction programme for all new staff to ensure that they fully understand both the school's Online Safety Policy and Acceptable Use Policy.
- The Online Safety Policy, Acceptable Use Policy, curriculum resources and general Online Safety issues are discussed regularly in staff/team meetings.

Online Safety– Raising parents/carers awareness

"Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it." (Byron Report, 2008).

Our school offers opportunities for parents/carers and the wider community to be informed about online safety, including the benefits and risks of using various technologies both at home and at school through:

- School newsletters, School Website and other publications
- Parents' evening interactive display on Online Safety
- Parents Online Safety Awareness sessions or workshops.
- Promotion of external Online Safety resources/online materials

Online Safety– Raising Governors' awareness

Governors, particularly those with specific responsibilities for online safety, ICT or child protection, are kept up to date through discussion at Governor meetings, head teachers report, attendance at Local Authority Training, CEOP or internal staff/parent meetings. NB: The Online Safety Policy is reviewed and approved by the governing body.

Evaluating the impact of the Online Safety Policy

There is a need to monitor and evaluate the impact of safeguarding procedures throughout the school. The headteacher and SLT are responsible for the monitoring and evaluation of safeguarding (including online safety) within Coupe Green Primary School. Individual staff are responsible for the recording and reporting of incidents

When monitoring takes place the school should consider:

- Is the Online Safety Policy having the desired effect?
- Are Online Safety incidents monitored, recorded and reviewed effectively?
- Is the introduction of new technologies risk assessed?
- Are these assessments included in the Online Safety Policy?
- Are incidents analysed to see if there is a recurring pattern e.g. specific days, times, classes, groups and individual children and how can these patterns be addressed most effectively e.g. working with a specific group, class assemblies, reminders for parents?
- How does the monitoring and reporting of Online Safety incidents contribute to changes in policy and practice?
- How are staff, parents/carers, children and governors informed of changes to policy and practice?
- How often are the AUPs reviewed and do they include reference to current trends and new technologies?

Appendix List

APPENDIX 1 – Coupe Green Image Consent Form

APPENDIX 2 - ICT Acceptable Use Policy (AUP) – Staff and Governor

APPENDIX 3 - ICT Acceptable Use Policy (AUP) - Supply Teachers

APPENDIX 4 - ICT Acceptable Use Policy (AUP) - Pupils Agreement

APPENDIX 5 – ICT Acceptable Use Policy (AUP) – Parent's Letter

APPENDIX 6 – Classroom Online Safety Rules (EYFS KS1)

APPENDIX 7 – Classroom Online Safety Rules (KS2)

APPENDIX 8 – Online Safety Incident Log

APPENDIX 9 – Responding to Online Safety Incident Escalation Procedures

Reviewed: January 2022

Appendix 1

IMAGES AND VIDEOS PARENTAL CONSENT FORM

We are required to seek consent to use images and videos of our pupils. This form explains the reasons why and how Coupe Green Primary School may use images and videos of your child. Please read the form thoroughly and outline your agreement as appropriate.

Name of pupil:	
Year Group:	

Why do we need your consent?

Coupe Green Primary School requests the consent of parents to use images and videos of their child for a variety of different purposes.

Without your consent, the school will not use images and videos of your child. Similarly, if there are only certain conditions under which you would like images and videos of your child to be used, the school will abide by the conditions you outline in this form.

Why do you we use images and videos of your child?

The school uses images and videos of pupils as part of school displays to celebrate school life and pupils' achievements; to promote the school on social media and on the school's website; and for other publicity purposes in printed publications, such as newspapers.

Where the school uses images of individual pupils, the full name of the pupil will not be disclosed. To celebrate children's work/achievements on Facebook a child's image and image of work may be accompanied by their first name only.

The school may take images or videos of individual pupils and groups of pupils to use on social media, the school website, in school prospectuses and other printed publications, such as a newsletter.

Who else uses images and videos of your child?

It is common that the school is visited by local media and press, who take images or videos of school events, such as sports days. Pupils will appear in these images and videos, and these may be published in local or national newspapers, or on approved websites.

The following organisations may use images and videos of your children:

- Lancashire Evening Post/Leyland Guardian
- Tempest Photography

Where any organisations other than those above intend to use images or videos of your child, additional consent will be sought before any image or video is used.

What are the conditions of use?

- This consent form is valid for as long as your child is a pupil at the school.
- It is the responsibility of parents to inform the school, in writing, if consent needs to be withdrawn or amended.
- The school will not use the personal details or full names of any pupil in an image or video, on our website, in our school prospectuses or any other printed publications.
- The school will not include personal emails or postal addresses, telephone or fax numbers on images or videos on our website, in our school prospectuses or any other printed publications.
- The school may use pictures of pupils and teachers that have been drawn by pupils.
- The school may use work created by pupils.
- The school may use group or class images or videos with general labels, e.g. 'sports day'.
- The school will only use images and videos of pupils who are suitably dressed, i.e. it would not be suitable to display an image of a pupil in swimwear.
- The school will take class images of your child which are available to purchase annually.

Providing your Consent

Please read the following conditions thoroughly and provide your consent as appropriate by ticking either 'Yes' or 'No' for each criteria.

The school will only publish images and videos of your child for the conditions that you provide consent for.

I PROVIDE CONSENT TO:	**YES**	**NO**
Using images of my child on the school website.		
Using videos of my child on the school website.		
Using images of my child on social media, currently Facebook.		
Using videos of my child on social media, currently Facebook.		
The local media using images of my child to publicise school events and activities (only including the organisations outlined above).		
The local media using videos of my child to publicise school events and activities (only including the organisations outlined above).		
Using images of my child in marketing material, e.g. the school brochure and prospectus.		
Sharing my child's name and class with a school-appointed external photography company for official school images.		

Refreshing your Consent

Consent will be refreshed where any changes to circumstances occur – this can include, but is not limited to, the following:

- New requirements for consent, e.g. an additional social media account will be used to share pupil images and videos
- Changes to a pupil's circumstances, e.g. safeguarding requirements mean a pupil's image cannot be used
- Changes to parental consent, e.g. amending the provisions for which consent has been provided for

Where you would like to amend the provisions for which consent has been provided, you must submit your request in writing to the headteacher. A new form will be supplied to you to amend your consent accordingly and provide a signature.

Withdrawing your Consent

Parents have the right to withdraw their consent at any time. Withdrawing your consent will not affect any images or videos that have been shared prior to withdrawal.

If you would like to withdraw your consent, you must submit your request in writing to the headteacher.

Declaration

I, _____(name of parent), understand:

- Why my consent is required.
- The reasons why Coupe Green Primary School uses images and videos of my child.
- Which other organisations may use images and videos of my child.
- The conditions under which the school uses images and videos of my child.
- I have provided my consent above as appropriate, and the school will use images and videos of my child in line with my requirements.
- I will be required to re-provide consent where any circumstances change.
- I can amend or withdraw my consent at any time and must do so in writing to the headteacher.

Name of parent: _____

Signature: _____

Date: _____

If you have any questions regarding this form, please do not hesitate to contact the school office.

Appendix 2

Coupe Green Primary School's - ICT Acceptable Use Policy
Staff and Governor Agreement

ICT and the related technologies such as email, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff and Governors are aware of their individual responsibilities when using technology. All staff members and Governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will be an active participant in Online Safety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, pupils or wider members into disrepute. This includes derogatory/ inflammatory comments made on Social Network Sites, Forums and Chat rooms.
5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
6. I will respect copyright and intellectual property rights.
7. I will ensure that all electronic communications with pupils and other adults are appropriate.
8. I will not use the school system(s) for personal use in working hours (except for use during breaks/lunchtimes.)
9. I will not install any hardware or software without the prior permission of the SMT.
10. I will ensure that personal data is kept secure at all times and is used appropriately in accordance with Data Protection legislation.
11. I will ensure that Images of pupils and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or per son/s in the image.
12. I will report any known misuses of technology, including the unacceptable behaviours of others.
13. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.
14. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
15. I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any

attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.

16. I understand that network activities and online communications may be monitored, including any personal and private communications made using school systems.
17. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.
18. I will take responsibility for reading and upholding the standards laid out in the AUP. I will support and promote the school's Online Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
19. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature ……..…….……

Date …….…….…….

Full Name ..…….…… (Please print)

Position/Role ……..……..……..

Appendix 3

Coupe Green Primary School's - ICT Acceptable Use Policy Supply teachers and Visitors/Guests Agreement

For use with any adult working/helping in the school for a short period of time.

- I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.

- I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.

- I will respect copyright and intellectual property rights.

- I will ensure that Images of pupils and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.

- I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.

- I will not install any hardware or software onto any school system.

- I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature ……..…….……

Date …….…….……

Full Name ……..……(PLEASE PRINT)

Position/Role……

Appendix 4

Coupe Green Primary School's- ICT Acceptable Use Policy Pupils Agreement / Online Safety Rules

These rules are a reflection of the content of our school's Online Safety Policy. It is important that parents/carers read and discuss the following statements with their child(ren), understanding and agreeing to follow the school rules on using ICT, including use of the Internet.

- I will only use ICT in school for school purposes.
- I will only use the Internet and/or online tools when a trusted adult is present.
- I will only use my class email address or my own school email address when emailing.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- I will not deliberately bring in inappropriate electronic materials from home.
- I will not deliberately look for, or access inappropriate websites.
- If I accidentally find anything inappropriate I will tell my teacher immediately.
- I will only communicate online with people a trusted adult has approved
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not give out my own, or others' details such as names, phone numbers or home addresses.
- I will not tell other people my ICT passwords.
- I will not arrange to meet anyone that I have met online.
- I will only open/delete my own files.
- I will not attempt to download or install anything on to the school network without permission.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my Online Safety.
- I understand that failure to comply with this Acceptable Use Policy may result in disciplinary steps being taken in line with the school's Behaviour Policy.

……..

Parent/ Carer signature

We have discussed this Acceptable Use Policy and ……..... (Please print child's name) agrees to follow the Online Safety rules and to support the safe use of ICT at Coupe Green Primary School.

Parent /Carer Name (Print) ……..…….

.

Parent /Carer (Signature) ……..…….

Class ……Date…….……

Appendix 5

ICT Acceptable Use Policy (AUP) – Parents' Letter
Coupe Green Primary School

Dear Parent/ Carer

The use of ICT including the Internet, email, learning platforms and today's mobile technologies are an integral element of learning in our school. To make this as successful and as beneficial as possible for all learners, we expect all pupils to act safely and responsibly when using technology both within, and outside of, the school environment.

This is particularly relevant when using Social Network Sites which are becoming increasingly popular amongst both the adult population and young people. However, many sites do have age restriction policies where the minimum acceptable age is 13 years. Any child who sets up or uses such a site and is below the acceptable age is in clear breach of these age-restriction policies and therefore we actively discourage this in our school.

The enclosed ICT Acceptable Use Policy forms part of the wider School Online Safety Policy and alongside the school's Behaviour Policy outlines those principles we expect our pupils to uphold for the benefit of both themselves and the wider school community.

Your support in achieving these aims is essential and I would therefore ask that you please read and discuss the enclosed ICT Acceptable Use Policy with your child and return the completed document as soon as possible.

Signing the School Acceptable Use Policy helps us to maintain responsible use of ICT and safeguards the pupils in school.

If you have any concerns or would like to discuss any aspect of the use of ICT in school, please contact the Hedateacher or any member of the school's Senior Leadership Team.

Yours sincerely

Mrs J Littlewood

Headteacher

Appendix 6
Online Safety Rules (EYFS/KS1)

Our Golden Rules for
Staying Safe with ICT

We only use the Internet when a trusted adult is with us.

We are always polite and friendly when using online tools.

We always make careful choices when we use the Internet.

We always ask a trusted adult if we need help using the Internet.

We always tell a trusted adult if we find something that upsets us.

Appendix 7
Online Safety Rules (KS2)

Our Golden Rules for Staying Safe with ICT

- We always ask permission before using the internet.
- We only use the Internet when a trusted adult is around.
- We immediately close/minimise any page we are uncomfortable with (or if possible switch off the monitor).
- We always tell an adult if we see anything we are uncomfortable with.
- We only communicate online with people a trusted adult has approved.
- All our online communications are polite and friendly.
- We never give out our own, or others', personal information or passwords and are very careful with the information that we share online.
- We only use programs and content which have been installed by the school.

Appendix 8

Online Safety Incident Log

Group: .....

Date	*Time*	*Incident*	*Action Taken*		*Incident Reported By*	*Signature*
			What?	*By Whom?*		

Monitoring Websites Log – carried out fortnightly by ICT Technician

Date	*Time*	*Lightspeed Activity Report completed by*	*Any incidents to be taken further?*	*Action Taken*		*Signature*
				What?	*By Whom?*	

Appendix 9

Responding to incidents of misuse – flow chart