EYNSHAM COMMUNITY PRIMARY SCHOOL

ONLINE SAFETY POLICY

THIS POLICY WAS AGREED BY GOVERNORS ON (DATE):	**May 2025**
REVIEW DATE:	**May 2027**
CHAIR OF GOVERNORS:	 **Peter Leonard**
Headteacher:	 **Ginny Bayliss**

This policy has been agreed in consultation with the whole school community's stakeholders, including the Governing Body, to ensure that it remains fit for purpose.

Eynsham Community Primary School Online Safety Policy

Contents

Eynsham Community Primary School Online Safety Policy

Online-Safety Co-ordinator – Nicola Edwards
Computing Co-ordinator – Tom Williams

Introduction

Technology is such a large part of everyone's lives in modern Britain, and the recent lockdowns have highlighted the advantages that technology can have in aiding our school to deliver the curriculum to the pupils at Eynsham Community Primary School. The school is determined to implement and maintain good quality online safety education to the pupils. As a result, our curriculum will equip our young people with the skills to access life-long learning and employment.

New technologies inspire children to be creative, communicate and learn. However, while the internet is a great resource, it is important that children and young people are protected from the risks they may encounter. Eynsham Community Primary School endeavours to highlight benefits and risks of using technology and provides Safeguarding and education for users to enable them to control their online experience.

Teaching and Learning

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in our school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

Opportunities for this learning will come across a child's education at Eynsham Community Primary School in the following ways:

- We will provide a curriculum/Jigsaw curriculum/other lessons which has e-Safety related lessons embedded throughout.
- We will celebrate and promote e-Safety through our curriculum, a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant e-Safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objective for specific curriculum areas.
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We will remind pupils about their responsibilities through an Acceptable Use Policy which every pupil will sign and be reminded of throughout the year in relation to online safety.
- School will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils will be guided to use age-appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- Pupils will be taught about the impact of online bullying and know how to seek help if they are affected by any form of online bullying. This is linked into the Jigsaw scheme of learning and linked to the schools Anti-Bullying Policy.

- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button.

Remote/Home Learning

As we discovered throughout the COVID pandemic, there is a need for online provision to be in place so that children can receive as close as possible, the education that they would do in school, online. Children will also use the online platform (Google Classroom) in order to complete homework, and access any learning as a result of school closure. In order to provide this, at Eynsham Community Primary School, we will provide the following guidelines to teachers as well as to children:

- We endeavour to ensure that pupils continue to receive a good level of education 'beyond the classroom' by providing a range of resources via Google Classrooms and other learning portals such as Times Table Rockstars.
- We expect pupils to follow the same principles, as outlined in the school's Acceptable Use policy, whilst learning at home.
- Any form of online learning will be treated like it would be if it was within a classroom. Children will be informed that each lesson will be recorded, and that children must follow the 'online learning agreement' (See Appendix A)
- There may be occasions where children would work 1:1 online, as part of an intervention or support group. If this is the case, lessons will be recorded for safeguarding of the children as well as the adult. All recordings and teaching will be done via Google Classroom. Again, pupils must uphold the same level of behavioural expectations, as they would in a normal classroom setting.
- Any significant behavioural issues occurring on any virtual platform must be recorded, reported and appropriate sanction imposed, which may include temporarily suspending access to group online learning. For all minor behavioural incidents, these should be addressed using the normal restorative approaches.
- Staff should be mindful that when dealing with any behavioural incidents, online, opportunities to discuss and repair harm will not be the same as if the child or young person was in school. Therefore, it may be necessary to have a discussion with the parents, regardless how minor the incident, to ensure the child is emotionally well supported

General Note for incident in school or online

- Urgent or serious incidents should be referred straight to the Executive Headteacher or Head of School, or a member of SLT who is a Designated Safeguarding lead ·
- If necessary, refer to the other related internal policies eg Anti-Bullying, Child Protection.
- Normal recording on CPOMS for anything which staff would deem as a safeguarding issue should continue. Entries should be factual and action/follow up recorded also.

Staff Training

Our staff at Eynsham Community Primary School receive regular information and training on e-Safety issues, as well as updates as and when new issues arise. As part of the induction process all staff receive information and guidance on the online Safety Policy , the school's Acceptable Use Policy and reporting procedures. All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of online-safety and know what to do in the event of misuse of technology by any member of the school community. All staff will be encouraged to incorporate online-safety activities and awareness within their curriculum areas, as well as through the computing curriculum.

Managing ICT Systems and Access

The school will work alongside the schools chosen IT management system (ICT123) in supporting the setup and online safety of the pupils who are logged in via the school system. The school will agree on which users should and should not have internet access and the appropriate level of access and supervision they should receive.
All users will sign an Acceptable Use Policy provided by the school, appropriate to their age and type of access. Users will be made aware that they must take responsibility for their use and behaviour whole using the school ICT system and that such activity will be monitored and checked.

At Key Stage 1, pupils will access the network using an individual username and a password which the teacher supervises. This will continue into Key Stage 2, however when the children reach Upper Key Stage 2 (Year 5), they will get the opportunity to set their own password. Teachers will remind children about the need to log out of the computer after each lesson.
Members of staff will access the internet using an individual username and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their ID or password. All internet activity is logged by the school's internet provider (ICT123). These logs may be monitored by authorised school staff.

Breaching of policy

A breach or suspected breach of policy by a School employee, contractor or pupil may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual. Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

Incident reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's Executive Headteacher/Head of School. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Executive Headteacher/Head of School. Pupil incident concerns must be passed on immediately (if serious) to a member of SLT. Bullying or racist incidents must be passed onto the Executive Headteacher/Head of School immediately and logged appropriately using CPOMS.

Computer Viruses

Staff must ensure that all files downloaded from the Internet, received via e-mail or on removable media must be checked for any viruses using school provided anti-virus software before using them.

- Never interfere with any anti-virus software installed on school ICT equipment that you use.
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your School ICT support.
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know

Email

Eynsham Community Primary School Online Safety Policy

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette. The Computing Curriculum states that children should use and be familiar with email. The feature of the children's accounts will be disabled for all pupils throughout the academic year, until the time that they need this feature for their computing lessons.

Managing emails

- The school gives all staff their own e-mail account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary, e-mail histories can be traced. The school email account should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.
- All e-mails should be written and checked carefully before sending, in the same way as any letter written on school headed paper.
- Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Executive Headteacher/Head of School or member of SLT.
- Pupils may only use school approved email accounts on the school system (Gmail) and only under direct teacher supervision when learning about this through the computing curriculum.
- E-mails created or received as part of your School job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:
  - Delete all e-mails of short-term value
  - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives
- All pupils will have their own individual school issued accounts.
- When they are switched on for teaching purposes, all pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission and virus check attachments.
- Staff must inform the Executive Headteacher or Head of School if they receive an offensive e-mail.
- However adults you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.

Sending Emails

Use your own school e-mail account so that you are clearly identified as the originator of a message and when necessary copy in a member of SLT e.g. if communicating with parents.

- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.

- School e-mail is not to be used for personal advertising.

Receiving emails

- Teachers email addresses should not be given out to parents, unless direct communication is necessary for a particular need, such as SEND or medical needs.

- Never open attachments from an untrusted source.

Emailing personal, sensitive, confidential or classified information

- Assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided where possible.
- The use of Hotmail, BT Internet, AOL or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted.

- Where your conclusion is that e-mail must be used to transmit such data:

  - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

    - Verify the details, including accurate e-mail address of any intended recipient of the information
    - Do not copy or forward the e-mail to any more recipients than is absolutely necessary

  - Send the information as an encrypted document **attached** to an e-mail
  - Provide the encryption key or password by a **separate** contact with the recipient(s)
  - Do not identify such information in the subject line of any e-mail
  - Request confirmation of safe receipt

When sending an e-mail containing personal or sensitive data you need to put a security classification in the first line of the e-mail. For e-mails to do with information about a pupil, for example, you need to put in **PROTECT – PERSONAL** on the first line of the e-mail.

This also needs to go on the top of any documents that you send (i.e. Word documents, Reports, Forms, including paper documents you send in hardcopy, etc). The name of the individual is not to be included in the subject line and the document containing the information encrypted. This provides additional security.

Equal Opportunities

Pupils with Additional Needs

Staff are aware that some pupils may require additional support including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of online Safety issues.

Where a pupil has limited social understanding, careful consideration is given to group interactions including nurture groups when raising awareness of online Safety. Internet activities are planned and well managed and differentiated appropriately for these children and young people.

Online safety – Roles and Responsibilities

As online Safety is an important aspect of strategic leadership within the school, the Executive Headteacher/Head of School and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. SLT and Governors are kept updated and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE.

Online safety in the curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for Online Safety guidance to be given to the pupils on a regular and meaningful basis. Online Safety is embedded within our curriculum and regularly referred to.

- The school has a framework for teaching internet skills in ICT lessons. This involves each year group teaching a unit of online safety throughout the academic year, as well as a refresher unit around online safety at the beginning of each long term.
- The school provides opportunities within a range of curriculum areas to teach about online Safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise as well as part of the online Safety curriculum.
- Pupils are taught about copyright and respecting other people's information, data, images, etc through discussion, modeling and activities.
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum.

Online Safety Skills development for staff

- Our staff receive updates and training on online Safety issues from the Computing Subject Leader.
- Subject leader to deliver Online safety workshops alongside outside agencies to inform parents around the dangers children are exposed to online.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of online Safety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowchart).
- All staff are encouraged to incorporate online Safety activities and awareness within their curriculum areas.

Misuse and Infringements

Complaints

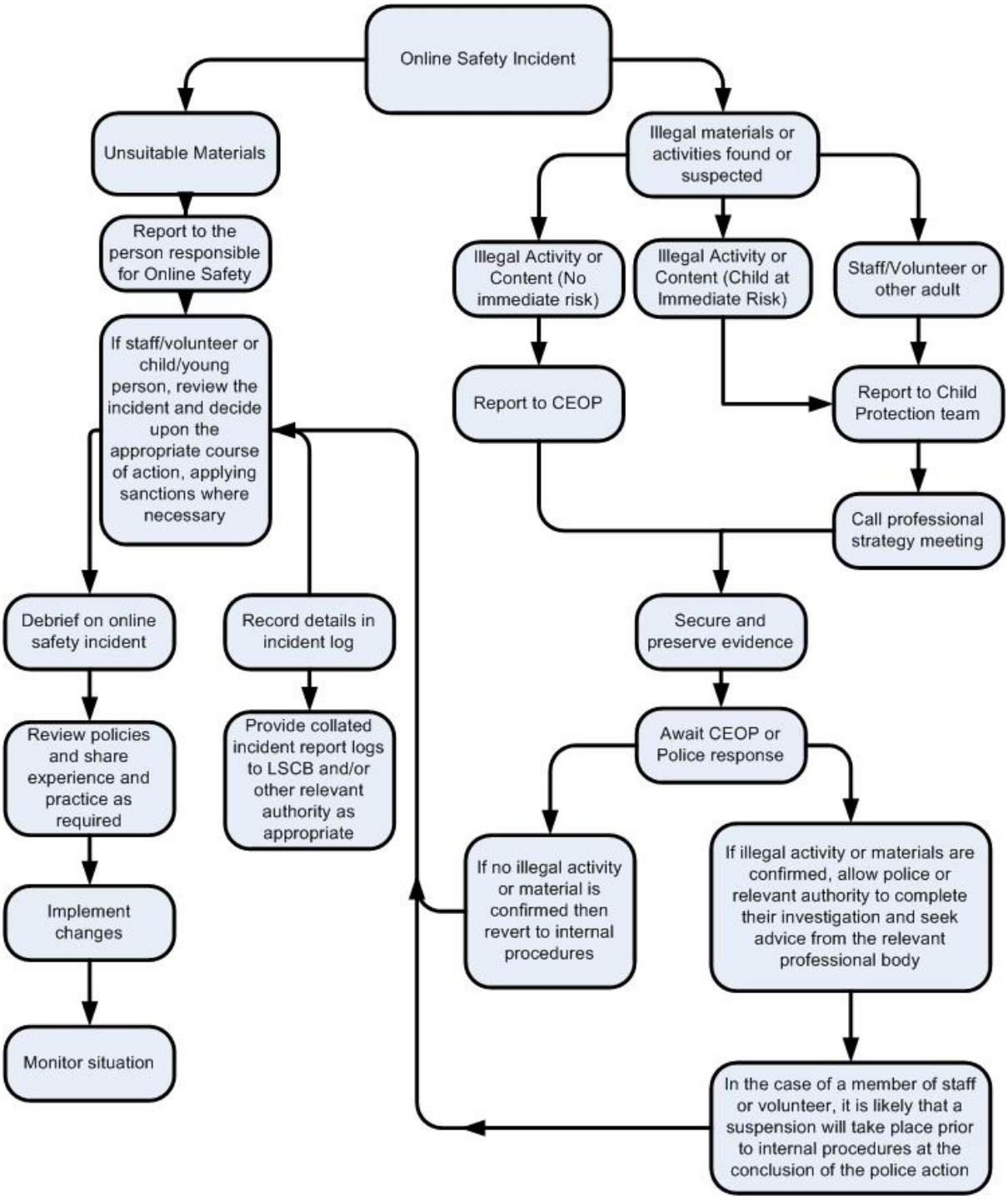
Complaints and/ or issues relating to online Safety should be made to the Executive Headteacher/Head of School. Incidents should be logged and the **Flowcharts for Managing an online Safety Incident** should be followed.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the online Safety co-ordinator

- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the online Safety co-ordinator, depending on the seriousness of the offence; investigation by the Executive Headteacher/Head of School, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)

Flowcharts for Managing an Online Safety Incident



Record of reviewing devices / internet sites (responding to incidents of misuse)

Group: .....

Date: .....

Reason for investigation: .....

.....

.....

.....

Details of first reviewing person

Name: .....

Position: .....

Signature: .....

Details of second reviewing person

Name: .....

Position: .....

Signature: .....

Name and location of computer used for review (for web sites)

.....

.....

Web site(s) address / device	Reason for concern

Conclusion and Action proposed or taken	

Internet Access

Managing the internet

- The school maintains students who will have supervised access to Internet resources (where reasonable) through the school's internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.

- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work.

- All users must observe copyright at all times.

Internet Use

- Do not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended audience.

- Don't reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog.

- On-line gambling or gaming is not allowed in school or on school ICT resources.

It is at the Headteacher/Head of School's discretion on what internet activities are permissible for staff and pupils and how this is disseminated.

Infrastructure

- Eynsham Community Primary School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; the EY General Data Protection Regulation (GDPR), The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.

- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required. This will only be activated throughout units of work which require the children to use email.

- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the class teacher.

- It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines

- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the network manager's to install or maintain virus protection on personal systems.

- Pupils are not permitted to download programs or files on school based technologies without seeking prior permission from the Executive Headteacher/Head of School or IT support team.

- If there are any issues related to viruses or anti-virus software, the network manager should be informed.

Social Networking Sites

- At present, the school endeavors to deny access to social networking sites to pupils within school

- We encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are. This is taught through the online safety units of work.

- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.

- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, email address, specific hobbies/ interests).

- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.

- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.

- Our pupils are asked to report any incidents, including ones that happen outside of school time, but involve children at the school, so that adults can be aware of this.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting online Safety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss online Safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ carers and pupils are actively encouraged to contribute to adjustments or reviews of the school online Safety policy.

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school

- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g. on school website)

- Parents/ carers are asked to sign an statement saying agreeing to follow the online Safety rules. (see Appendix 2)

- The school disseminates information to parents relating to online Safety where appropriate in the form of;

    - Information and celebration evenings
    - Posters
    - Website/ Learning Platform postings
    - Newsletter items

Passwords Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Year 5 pupils will get eh chance to change their password to something they can remember at the start of the year. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's online Safety Policy and Data Security

- Users are provided with an individual network, email and Management Information System (where appropriate) log-in username.

- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.

- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations/laptops/ipads are locked if left unattended.

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment

- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on trips. However with the express permission of the Headteacher/Head of School, images can be taken provided they are transferred immediately and solely to the schools network and deleted from the staff device.

- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on trips.

- If pupils bring a mobile phone or similar device into school, it should be handed into the office at the start of the day and returned to the owner at home time.

Publishing pupils images and work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- On the school web site

- In the school prospectus and other printed publications that the school may produce for promotional purposes

- Recorded/ transmitted on a video

- In display material that may be used in the school's communal areas

- In display material that may be used in external areas, i.e. exhibition promoting the school

- General media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time.

Pupils' surnames will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published.

Storage of Images

- Images/ films of children are stored on the school's network.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher/Head of School.
- Staff must use password protected USB sticks if they wish to store / transfer images.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network.
- The administrator has the responsibility of deleting the images when they are no longer required.

School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

- As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you.
- The school business manager will log ICT equipment issued to staff and record serial numbers as part of the school's inventory.
- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT Facilities if available.
- Ensure that all ICT equipment that you use is kept physically secure.
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990.
- It is imperative that you save your data on a frequent basis to the school's network drive, or automatically via the cloud drive. You are responsible for the backup and restoration of any of your data that is not held on the school's network drive.
- Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted.
- It is recommended that a time locking screensaver is applied to all machines. Any PCs etc accessing personal data must have a locking screensaver as must any user profiles.
- Privately owned ICT equipment should not be used on a school network?
- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled.
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.
- All redundant ICT equipment is disposed of in accordance with Waste Electrical

Portable & Mobile ICT Equipment

This section covers such items as laptops, ipads, PDAs and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on School systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on school's network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop / ipad in the boot of your car before starting your journey.
- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis.
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.
- The installation of any applications or software packages must be authorised by the computing subject leaders, fully licensed and only carried out by your ICT support.
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.
- Portable equipment must be transported in its protective case if supplied.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that they are used appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. These must be kept in cupboards in classrooms. If a mobile phone is to be used it must be in child free areas e.g. the staff room or office or at breaks and lunchtimes. Only in exceptional circumstances should a member of staff contact a pupil or parent/carer using their personal device.
- Under no circumstances should staff use their mobile phone during learning time or in areas that pupils have access to.
- Pupils are not allowed to bring personal mobile devices/phones to school unless permission has been given by Parents and Staff members. If they are brought in as a safety feature e.g. the child is walking home alone, the phone will be signed into the office at the start of the day and signed out at home time.
- The school is not responsible for the loss, damage or theft of any personal mobile device.

- The sending of inappropriate text messages between any members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Acts Relating to Monitoring of Staff email

The EU General Data Protection Regulation (GDPR)

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. It expands the rights of individuals to control how their personal data is collected and processed.

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

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Human Rights Act 1998

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent:

there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another persons password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Key Stage One Pupil Acceptable Use

Agreement / Online Safety Rules

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment

- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet

Signed (child): .....

Signed (parent): .....

Key Stage Two Pupil Acceptable Use

Agreement / Online Safety Rules

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or offensive. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details, such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and that my parent/ carer may be contacted if a member of school staff is concerned about my online Safety.

Signed ……..Date…….

Eynsham Community Primary School Online Safety Policy

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies, etc is an integral important part of learning in our school. We expect all children to be safe and responsible when using any ICT.
Please read and discuss these online Safety rules with your child and return the slip at the bottom of this page

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or offensive. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details, such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and that my parent/ carer may be contacted if a member of school staff is concerned about my online Safety.

✂----------

Parent/ carer signature
We have discussed this and …….....(child name) agrees to follow the online Safety rules and to support the safe use of ICT at Eynsham CP School.

Parent/ Carer Signature …….

Class …….. Date ……

Eynsham Community Primary School Online Safety Policy

Staff, Governor and Visitor

Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT.

All staff are expected to sign this policy and adhere at all times to its contents.

Any concerns or clarification should be discussed with the Headteacher/Head of School.

- I will only use the school's email, Internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils or parents.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software without permission of the Headteacher/Head of School.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or the Executive Headteacher/Head of School.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- I understand that all my use of the Internet and other related systems can be monitored and logged and can be made available, on request, to my line manager or Executive Headteacher/Head of School.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute, this includes my use of any social media.
- I will support and promote the school's online Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

- I understand this forms part of the terms and conditions set out in my contract of employment.

User Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …… Date ……

Full Name ……(printed)

Job title . . . . . .

Appendix A
Code of Conduct for
Google Classrooms/Live Meets/Hang outs

Google Classrooms is now being used by all class teachers at Eynsham Primary School as a way to facilitate online learning and to engage with children during classroom live meets.

We would ask that all children have read and follow the basic rules whilst using this facility.

- Make sure your family know that you are using Google classrooms and when any live meets are taking place.
- Be in an appropriate room and wear appropriate clothing.
- Live meets are only to be organised by a teacher.
- Your teacher will be the last person to leave the Google Meet. Do not attempt to re-enter once you have left.
- If you want to chat with friends, please ask your parents to organise this privately and not through the school's Google Classrooms/Meets/Chat functions.
- All live meets will be recorded in case there is any issue and your teacher will remind you of this at the start of every session.
- Any videos that are uploaded on to Google classrooms are for teaching purposes only and must not be shared or copied.