Eyres Monsell
Primary School

eSafety Policy
2025 – 2026

Approved by **Date**	FSGP Committee February 2025
Review date	January 2026
Signed (Chair of Governors)	

Contents

Introduction

Eyres Monsell Primary School recognises the Internet and other digital technologies provide a vast opportunity for children and young people to learn. The Internet and digital technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.

As part of our commitment to learning and achievement we at Eyres Monsell Primary School want to ensure that the Internet and other digital technologies are used to:

- Raise educational standards and promote pupil achievement.
- Develop the curriculum and make learning exciting and purposeful.
- Enable pupils to gain access to a wide span of knowledge in a way that ensure their safety and security.
- Enhance and enrich their lives and understanding.

To enable this to happened we have taken a whole school approach to E- safety, which includes the development of policies and practices, the education and training of staff and pupils and the effective use of the School's ICT infrastructure and technologies.

Eyres Monsell Primary School, as part of this policy, holds steadfastly to the ethos that there should be an equitable learning experience for all pupils using ICT technology within the school. We recognise that ICT can allow all pupils, including disadvantaged and disabled pupils, increased access to the curriculum and other aspects related to learning.

Eyres Monsell Primary School is committed to ensuring that all its pupils, where technologically feasible and within the prevailing financial climate, will be able to use existing, as well as up and coming technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents, are educated as to the risks that exist so that they can take an active part in safeguarding children.

For the purposes of this document, Internet usage means any connection to the Internet via web browsing, external email, news groups or messaging services, mobile technologies e.g. mobile phone, including Bluetooth applications, PDA's etc.

Scope of Policy

The policy applies to:

- all pupils
- all teaching and support staff (including peripatetic), school governors and volunteers
- all aspects of the school's facilities where they are used by voluntary, statutory or community organisations

Eyres Monsell Primary School will ensure that the following elements are in place as part of its safeguarding responsibilities to pupils:

- a list of authorised persons who have various responsibilities for E- safety (DSL and Deputy DSLs, Computing Lead, Computer technician)
- a range of policies including acceptable use policies that are frequently reviewed and updated; information to parents that highlights safe practice for children and young people when using the Internet and other digital technologies
- adequate training for staff and volunteers
- adequate supervision of pupils when using the Internet and digital technologies
- education that is aimed at ensuring safe use of Internet and digital technologies
- use of policies for reporting/auctioning sanctions for abuse and misuse.

Infrastructure and Technology

Partnership working

Eyres Monsell Primary School recognises that as part of its safeguarding responsibilities we should strive to have a commitment to partnership working, we fully support and will continue to work with all stakeholders including staff, pupils, families and governors, to ensure that pupil and staff usage of the Internet and digital technologies is safe.

Eyres Monsell Primary School will, as part of its wider safeguarding responsibilities, seek to ensure that voluntary, statutory and community organisation take an approach to their activities that see the welfare of the child as paramount. To this end, we expect any organisation using the school's ICT or digital technologies to have appropriate policies and procedures that are aimed at safeguarding children and young people and reporting concerns.

Use of Internet facilities, mobile and digital technologies

Eyres Monsell Primary School will seek to ensure that Internet, mobile and digital technologies are used effectively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk.

Eyres Monsell Primary School expects all staff and pupils to use the Internet, mobile and digital technologies responsibly and strictly according to the conditions below. These expectations are also applicable to any voluntary, statutory and community organisations that makes use of the school's ICT facilities and digital technologies.

Users shall not:

Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children

- Promoting discrimination of any kind, promoting racial or religious hatred or promoting illegal acts.
- Any other information which may be offensive to peers or colleagues e.g. abusive images; promotion of violence; violent extremism, gambling; criminally racist or religious hatred material.

The School recognises that in certain planned curricular activities, searches relating to historical, scientific or current global events, may flag up through our monitoring and filtering systems. In such circumstances, the Senior Leadership Team will liaise with classroom staff to ensure that these are legitimately linked to the learning focus.

Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the Police:

- Images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative)
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist or anti-religious material
- Violence and bomb making/suspicious device making or plans
- Illegal taking or promotion of drugs
- Software piracy, including use of DVD technology Any other criminal activity

In addition, users may not:

- Enter into any personal transaction that involves the school network/connection or Local Authorities in any way;
- Visit sites that might be defamatory or incur liability on the part of the school network/connection or Local Authorities
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of the school network/connection (other than authorised and licensed automatic updates via the network / Internet e.g. Microsoft, Adobe etc.)
- Reveal or publicise confidential or proprietary information, which includes but is not limited to: financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships;
- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet;
- Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate. (e.g. Facebook etc.)
- Transmit unsolicited commercial or advertising material either to other user organisations, or to organisations connected to other networks, save where the material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe.
- Assist with unauthorised access to facilities or services accessible via the school network/connection.

- Access the devices, accounts, E-mail or applications designated to another individual or knowingly access information belonging to another individual without prior permission.
- Access or give access to another individual's login or password to access devices, emails or the school network.
- Undertake activities with any of the following characteristics:
    - Wasting staff effort or networked resources, including time on end systems accessible via the network and the effort of staff involved in support of those systems;
    - corrupting or destroying other users' data;
    - Violating the privacy of other users;
    - Disrupting the work of other users;
    - Using the network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
    - Continuing to use an item of networking software or hardware after EMPS has requested that use cease because it is causing disruption to the correct functioning of the school network/connection;
    - other misuse of the school network/connection, such as introduction of viruses.

    - Use any mobile or digital technologies or mobile Internet services in any way to intimidate, threaten or cause harm to others. Moreover, mobile technologies should not be used to access inappropriate materials or encourage activities that are dangerous or illegal.

Where EMPS/school network providers/connection provider become aware of an illegal act or an attempted illegal act, they will have to comply with the law as it applies and will take action directed by the police if a Regulation of Investigatory Powers Act (RIPA) Notice is issued.

Reporting Abuse

There will be occasions when either a pupil or an adult within the school receives an abusive email or accidentally accesses a website that contains abusive material. When such a situation occurs, the expectation of the school is that the pupil or adult should report the incident immediately to an appropriate person.

The School also recognises that there will be occasions where pupils will be victims of inappropriate behaviour that could lead to possible or actual significant harm. The response of the School will be to take the reporting of such incidents seriously and where judged necessary, the Designated Senior Person for Child Protection (DSL or Deputy DSL in the absence of DSL) within the School will refer details of an incident to the lead agencies involved in safeguarding children, namely Children's Social Care and the Police.

The School, as part of its safeguarding duty and responsibilities will assist and provide information and advice in support of child protection enquiries and criminal investigations.

Education and Training

Eyres Monsell Primary School recognises that the Internet and other digital technologies can transform learning; help to improve outcomes for children and young people; promote creativity; all of which add up to a more exciting and challenging classroom experience. As part of achieving this,

we want to create within Eyres Monsell Primary School an accessible system, with information and services online, which support personalised learning and choice. However, we realise that it will be necessary for our pupils to have the skills of critical awareness, digital literacy and good online citizenship to enable them to use the Internet and other digital technologies safely.

To this end, Eyres Monsell Primary School will:-

- Enable all pupils to exercise the skills of critical awareness, digital literacy and good online citizenship as part of the school curriculum.
- Educate school staff so that they are equipped to support pupils in gaining positive experiences when online and can help pupils develop strategies if they encounter a problem.
- Support parents in gaining an appreciation of Internet safety for their children and provide them with relevant information on the policies and procedures that govern the use of Internet and other digital technologies within the school and offer support in understanding how to keep their children safe online when using technology at home.

Standards and Inspection

Eyres Monsell Primary School recognises the need to have regular inspections of policies and procedures in order to ensure that its practices are effective and that the risks to pupils are minimised.

Monitoring

Monitoring the safe use of the Internet and other digital technologies goes beyond the personal use of the Internet and electronic mail a pupil or member of staff may have. Eyres Monsell Primary School recognises that in order to develop an effective whole school E-safety approach there is a need to monitor patterns and trends of use inside school and outside school (Education and Inspections Act 2006, Section 89(5)).

With regard to monitoring trends, within the school and individual use by school staff and pupils, Eyres Monsell Primary School will audit the use of the Internet and electronic mail in order to ensure compliance with this policy. The monitoring practices of the school are influenced by a range of national and Local Authority guidance documents and will include the monitoring of content and resources by the use of Policy Central.

Another aspect of monitoring, which our school will employ, is the use of mobile technologies by pupils, particularly where these technologies may be used to cause harm to others, e.g. bullying (see anti-bullying policy for further information). We will also ensure that school staff understand the need to monitor our pupils, and where necessary, support individual pupils where they have been deliberately or inadvertently been subject to harm.

The school's internet, network and ICT systems and subscriptions to services should be used with the utmost professionalism at all times. The school will aim to provide its staff with secure systems which will have filtering, monitoring and virus protection included. Anyone with access to the systems should be aware that their use of the systems is monitored, and this can be used to form evidence should any suspected infringements occur.

Sanctions

Where there is inappropriate or illegal use of the Internet and digital technologies, the following sanctions will be applied:

Child / Young Person

The child/young person will be disciplined according to the behaviour policy of the school, which could ultimately include the use of Internet, apps and email being withdrawn.
Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

Adult (Staff and Volunteers)

The adult may be subject to the disciplinary process, if it is deemed he/she has breached the policy
Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

If inappropriate material is accessed, children are taught to immediately turn off the monitor and report to an adult. Adult to then report to a member of the ICT team or a member of SLT. Member of ICT to contact filtering services and teacher/ Deputy Headteacher Pastoral or SLT to speak to the child concerned and their parents. Incident to be logged on CPOMS and reported to the Headteacher. As part of the schools Long Term Plans, every class will participate in half termly esafety lessons.

Working in Partnership with Parents and Carers

Eyres Monsell Primary School is committed to working in partnership with parents and carers and understands the key role they play in the Internet safety of their children, through promoting Internet safety at home and elsewhere.

We at Eyres Monsell Primary School also appreciate that there may be some parents who are concerned about the use of the Internet, email and other digital technologies in school. In such circumstances, school staff will meet with parents/carers to discuss their concerns and agree upon a series of options that will allow their child to fully access the curriculum, whilst remaining safe.

Appendices of the E-safety Policy

There are multiple aspects of the school's E-safety policy, which include acceptable use policies for both staff and pupils, data security and retention and use of social media.

APPENDIX A ACCEPTABLE USE AGREEMENT Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:	
When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I: • Will not access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Will report inadvertent use of a violent, criminal or child pornographic nature at home either by myself or by somebody in my household • Will not use them in any way which could harm the school's reputation • Will not access social networking sites or chat rooms • Will not use any improper language when communicating online, including in emails or other messaging services • Will not install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Will not share my password with others or log in to the school's network using someone else's details • Will not share confidential information about the school, its pupils or staff, or other members of the community • Will not access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	Date: