Blewbury Endowed C of E Primary School
Westbrook Street, Blewbury, Didcot, Oxon. OX11 9QB
Telephone: (01235) 850411

Online Safety Policy

Approved by Headteacher	**Signature**	**Date**
Jo Reeder		**28/11/23**
Approved by Chair of Governors	**Signature**	**Date**
Ann Parham		**28/11/23**
Date of Issue	November 2023	
Date of this review	November 2023	
Next review due	November 2025	

Our school is a place for all to belong. Through **love**, we nurture all to grow in their own unique way. We create an environment for all to flourish; to **forgive**, be **resilient** and **courageous**, making a difference to our community and the world beyond.

Nurture • Grow • Flourish

Scope of the policy

"It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate." KSCIE 2023.

This policy is written in line with 'Keeping Children Safe in Education' 2023 (KCSIE), 'Teaching Online Safety in Schools' (updated In January 2023) and other statutory documents. It complements subjects including Personal, Social and Health Education, Relationships and Sex Education and Computing. It also sits alongside our school's statutory Safeguarding and Child Protection Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

The updated version of 'Keeping children safe in education' in 2023 states that the breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism;

- contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.

- **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

- commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/ carers, visitors, governors) who have access to and are users of school ICT systems, both in and out of school.

The purpose of this policy statement is to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices.
- provide staff and volunteers with the overarching principles that guide our approach to online safety.
- facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help the safeguarding and senior leadership team to have a better understanding and awareness of filtering and monitoring through effective collaboration and communication with technical colleagues.
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

Roles and Responsibilities

The following section outlines the Online Safety roles and responsibilities of individuals and groups within the school:

Governors will:

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board. This will be carried out by the Governors receiving information about online safety incidents and monitoring reports.
- Support the school in encouraging parents and the wider community to become engaged in online safety activities.

Headteachers and Leaders will:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Ensure staff undergo safeguarding training (including online safety) at induction and with regular updates.
- Ensure governors and trustees undergo safeguarding and child protection training and updates (including online safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the nature and effectiveness of the school's arrangements.
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles.
- Liaise with technical colleagues regularly to have an understanding and awareness of filtering and monitoring provisions and manage them effectively – understand what is blocked or allowed for whom, when, and how. KSCiE 2023 places particular emphasis on robust filtering and monitoring systems and the DfE has made additional guidance available to support schools.
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information.
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident.
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised.
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety.
- Ensure the school website meets statutory requirements
- Ensure KCSIE 'Part 5: Sexual Violence & Sexual Harassment' is understood and followed throughout the school and that staff adopt a zero-tolerance, whole school approach to all forms of child-on-child abuse, and don't dismiss it as banter (including bullying).

- Be aware of the procedures to be followed in the event of a serious E Safety allegation being made against a member of staff.

The Headteacher alongside other Senior Leaders are responsible for ensuring that relevant staff receive suitable training to enable them to carry out their roles with regard to ensuring online safety.

<u>The Computing Lead will:</u>

• take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents.

• ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.

• provide training and advice for staff

• liaise with school technical staff

• liaise with members of the Senior Leadership Team to discuss reports of online safety incidents and creates a log of incidents to inform future online safety developments

• report to the Senior Leadership Team

<u>Network Manager / Technical staff (123ICT):</u>

The Network Manager is responsible for ensuring:

• that the school's technical infrastructure is secure and is not open to misuse or malicious attack.

• that the school meets required Online Safety technical and statutory requirements that may apply.

• that users may only access the networks and devices through properly enforced security protocols.

• the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person

• that they keep up to date with online safety technical information to effectively carry out their role and to inform and update others as relevant

• that the use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Senior Leaders / Computing Lead for investigation and action

• that monitoring software / systems are implemented and updated as agreed in school policies

- Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology. KCSIE (2023) sets out a greater understanding of technology and its role in safeguarding, so help DSLs and SLT to understand systems, settings and implications.

- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc
- Maintain up-to-date documentation of the school's online security and technical procedures.
- To report online-safety related issues that come to their attention in line with school policy.

- Work with the Headteacher to ensure the school website meets statutory DfE requirements.

Teaching and Support Staff

Are responsible for ensuring that:

• they have an up-to-date awareness of Online Safety matters and of the current school Online Safety Policy and practices

• they have read, understood this and related policies

• they report any suspected misuse or problem to the Headteacher / Senior Leader/ Computing Lead for investigation

• all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems

• Online Safety issues are embedded in all aspects of the curriculum and other activities

• pupils understand and follow and rules around acceptable use of technology

• pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

• they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices

• in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

The PSHE lead will:

- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHRE curriculum. This will include education on positive, healthy and respectful online relationships, the effects of their online actions on others and knowing how to recognise respectful behaviour online. Throughout these subjects, teachers should address online safety and appropriate behaviour in an age-appropriate way that is relevant to their pupils' lives.

The Designated Safeguarding Lead will

- be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

• sharing of personal data

• access to illegal / inappropriate materials

• inappropriate on-line contact with adults / strangers

• potential or actual incidents of grooming

• cyber-bullying

- Where they are not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised.
- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents.

Pupils will:

• be responsible for using the school digital technology systems in line with instruction from school staff

• understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

• be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.

• understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local Online Safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good Online Safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events.

Education and Curriculum

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in Online Safety is therefore an essential part of the school's Online Safety provision. Children need the help and support of the school to recognise and avoid Online Safety risks and build their resilience. Online Safety should be a focus in all areas of the curriculum and staff should reinforce Online Safety messages across the curriculum. The Online Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

• A planned Online Safety curriculum should be provided as part of Computing / PSHRE / other lessons and should be regularly revisited

• Key Online Safety messages should be reinforced as part of a planned programme of assemblies.

• Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

• Pupils should be helped to understand the need for pupil Acceptable Use Agreements and encouraged to adopt safe and responsible use both within and outside school.

• Staff should act as good role models in their use of digital technologies the internet and mobile devices

• In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

• Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Technical – infrastructure / equipment, filtering and monitoring

The school, along with 123ICT, will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their Online Safety responsibilities.

• School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.

• There will be regular reviews and audits of the safety and security of school technical systems.

• Servers, wireless systems and cabling must be securely located and physical access restricted

• All users will have clearly defined access rights to school technical systems and devices.

• All users will be provided with a username and secure password. Users are responsible for the security of their username and password.

• The administrator passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place.

• The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.

• Internet access is filtered for all users. Content lists are regularly updated and internet use is logged and regularly monitored.

• Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.

• An appropriate system is in place for users to report any actual / potential technical incident / security breach to the Network Manager.

• Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

• An agreed policy is in place for the provision of temporary access of “guests” (e.g., trainee teachers, supply teachers, visitors) onto the school systems.

• An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies

Mobile technology devices may be provided by the school and might include: iPad, tablet, laptop that usually has the capability of utilising the school's wireless network. All users should understand that the primary purpose of the devices in a school context is educational.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

• When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

• Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / local press. Parents / carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

• Staff and volunteers are allowed to take digital / video images to support educational aims. These images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.

• Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

•Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

• Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Communications

When using communication technologies, the school considers the following as good practice:

• The official school email service may be regarded as safe and secure and is monitored. Staff should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).

• Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

• Any digital communication between staff and pupils or parents / carers (email, blogs etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.

• Pupils should be taught about Online Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

• Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Handling online-safety concerns and incidents

- It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing and PSHRE).
- General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the online-safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.
- Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).
- School procedures for dealing with online safety will be mostly detailed in the following policies (primarily in the first key document):

    - Safeguarding and Child Protection Policy
    - Peer on Peer Abuse Policy
    - Anti-Bullying Policy
    - Behaviour Policy
    - Acceptable Use Policies
    - Prevent Risk Assessment
    - Data Protection Policy

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

• Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported. Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

• It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

• Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

• Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following: o Internal response or discipline procedures o Involvement by Local Authority or national / local organisation (as relevant). o Police involvement and/or action

• If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material o promotion of terrorism or extremism o other criminal conduct, activity or materials

• Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation. It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with in accordance with the school behaviour policy.