Ellwood Community Primary School

Believe, Achieve, Belong

E-Safety Policy

Date reviewed: July 2023 Next renew date: July 2025

Contents Page

1. Introduction

At Ellwood Community Primary School, we recognise that internet, mobile and digital technologies provide positive opportunities for children and young people to learn, socialise and play but they also need to understand the challenges and risks. At Ellwood Community Primary School, we understand that the digital world is an amazing place but with few rules, therefore our Computing curriculum allows teachers to provide children with the knowledge and critical thinking skills to keep themselves safe when using the internet and digital devices. We also understand the necessity of participation in national events to promote positive online behaviour such as Safer Internet Day.

Technology is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that all pupils, staff and governors will be supported to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Members of staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

The 4 key categories of risks:

Our approach to online safety is based on addressing the following categories of risk:

1. **Content** – being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-semitism, radicalisation, and extremism
2. **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
3. **Conduct** - 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
4. **Commerce** – risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/)

This policy should be read in conjunction with the following school policies and documents:

Acceptable Use for staff, Anti-Bullying and Hate Crime, Behaviour Policy, Complaints Policy, Child Protection and Safeguarding Policy, Data Protection Policy, Equal Opportunities Policy, Health and Safety Policy, Computing Policy, Life Skills policy and Relationships and Sex Education [RSE] policy.

2. Legislation and Guidance

This policy is based on the Department for Education's (DFE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in school
- UK council for Internet Safety (UKCIS) guidance: Education for a connected world

- UKCIS guidance: Sharing nudes and semi-nudes: advice for education settings working with children and young people
- The UKCIS external visitors guidance will help schools and colleges to ensure the maximum impact of any online safety sessions delivered by external visitors.
- Harmful online challenges and online hoaxes - this includes advice on preparing for any online challenges and hoaxes, sharing information with parents and carers and where to get help and support.

Government Guidance:

The Online Safety Bill 2022

The Online Safety Bill is a new set of laws to protect children and adults online. It will make social media companies more responsible for their users' safety on their platforms.

3. Monitoring and Reviewing of this policy

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

There will be an on-going opportunity for staff to discuss with the E-safety lead any issue of E-safety that concerns them. Due to the ever changing nature of ICT, the school will review this policy annually and consideration given to the implications for future whole school development planning. The policy will be amended if new technologies are adopted or Central Government changes the orders of guidance in any way.

4. Roles and Responsibilities

It is the role of the E-Safety lead to keep abreast of current issues and guidance through maintaining a working knowledge of the responsibilities outlined in Keeping Children Safe in Education (2023) and also through the guidance of organisations such as Gloucestershire LA, CEOP (Child Exploitation and Online Protection) and Child Net.

Staff and Governors are kept updated by the E-Safety Lead and understand the issues and strategies at our school in relation to local and national guidelines and advice.

All members of staff at Ellwood Community Primary School, understand their day-to-day responsibility of keeping the children in their care safe online. They receive regular information and training on E-Safety issues and have been made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety. New staff receive information on the school's Acceptable User Agreement as part of their induction. E-Safety is addressed in staff meetings to ensure that training and updates remain relevant and current to all staff.

Ellwood Community Primary School identifies that there is a clear duty to ensure that all children are protected from potential harm online. The Headteacher and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. All breaches of this policy must be reported to the Headteacher.

5. E-Safety in the curriculum

E-Safety is fully embedded within our curriculum. At Ellwood Community Primary School, we provide an age appropriate curriculum for online safety which enables pupils to become informed, safe and responsible. Our Life Skills and the Computing curriculum are central in supporting the delivery of online safety

education. The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by these technologies. E-Safety learning will include areas such as:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing e.g. regulated screen time and diverse online activity

- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment

- Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives), understanding the dangers of giving out personal details online and the importance of maintaining maximum privacy online

- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others

- Understanding digital footprints of all online postings and conversations

- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images

- Understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help

- How the law can help protect against online risks and abuse.

It is a statutory requirement for all schools to teach:

KS1 Pupils:

- Use technology purposefully to create, organise, store, manipulate and retrieve digital content
- Recognise common uses of information technology beyond school
- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

KS2 Pupils:

- Understand computer networks, including the internet; how they can provide multiple services, such as the World Wide Web, and the opportunities they offer for communication and collaboration
- Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content
- Use technology purposefully to create, organise, store, manipulate and retrieve digital content
- Recognise common uses of information technology beyond school
- Use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

6. Password Security

Password security for staff members

Password security is essential for staff, particularly as they are able to access and use pupil data. Members of staff are expected to have secure passwords which are not shared with anyone. Staff are reminded regularly the need for password security and the secure locking of devices when not in use.

Password security for children

Pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Pupil are regularly of reminded of the need for password security and the secure locking of devices when not in use.

All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's E-safety Policy.

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

If a user thinks their password may have been compromised or someone else has become aware of their password, this must be reported to the school office.

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 are not left unattended in a logged-on state.

Teacher iPads are password protected. These are not shared with the children and must be logged into by an adult.

7. Managing the internet safely

Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Ellwood Community Primary School expects everyone to use internet, mobile and digital

technologies responsibly and strictly according to the conditions set out in this policy. The school uses South West Grid for Learning (SWGfL) to filter the internet and staff are alerted to any breaches.

- The school maintains students will have supervised access to internet resources (where reasonable) through the school's internet technology.
- Staff will preview any recommended sites, software and apps before use.
- Raw image searches are discouraged when working with pupils.
- If internet research is set for homework, specific sites shared will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

Infrastructure

- School internet access is controlled through the SWGfL web filtering service.
- We are aware of its responsibility when monitoring staff communication under current legislation
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off closed and the incident reported immediately to the nearest member of staff and to the E-Safety Lead as soon as possible.
- 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. If pupils wish to bring in work on removable media it must be given to the class teacher for a safety check first.

8. Managing other web

- At present, the school endeavours to deny access to social networking sites to pupils within school.
- Staff must ensure that any online activity (including use of social media), both in school and outside school, will not bring their professional role into disrepute.
- 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.
- 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.
- Members of staff are expected 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 and staff are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils and staff are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils and staff are asked to report any incidents of cyber-bullying to the school.

9. Mobile Phones

- All visitors to leave their mobile phones in the office locker
- Mobile phones must not be used in view of the children unless permission has been agreed by a member of SLT.
- Mobile phones must not be used and shared in any way with the children.

- The staff room has been designated a 'safe place' for members of staff to use their devices.
- Only in special circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device.
- Members of staff may use personal mobile device on a school trip for communication calls only.
- Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child, unless there is a pre-specified permission from the Headteacher.
- Pupils in Year 5 or 6 who walk home from school by themselves are able to bring a mobile phone into school. If children bring a device into school it must be switched off and handed to the office on entry into school and will not be allowed to be used during the school day. The phone must then be collected at the end of the school day. If a child in needs to bring a mobile phone into school, their parent or carer must ask permission from the Headteacher.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- Smart Watches (without independent connectivity and cameras) may be worn by staff providing they are being used as normal watches and for no other function beyond telling the time.
- The sending of inappropriate text messages between any members of the school community is not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

10. Managing emails

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email 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 email in relation to their age and good 'etiquette'.

The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed. This account must be used for all data relating to the fulfilment of our role as educators. This also includes governors.

- 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 email histories can be traced. This 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 email addresses.
- E-mails sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes. All children use a class or group email address.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (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. Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform the Headteacher if they receive an offensive e-mail.
- Pupils are introduced to emailing as part of the Computing Scheme of Work

11. Safe use of images

Taking of Images and Film

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. Digital images are easy to capture, reproduce and publish and, therefore, misused. 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. In line with GDPR, with the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupil. These must only be taken on school cameras, iPads, iPods or other school devices. Photographs and images of pupils are only stored on the school's agreed secure networks which include some cloud based services.

Publishing pupils' images and work

All parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- on the school's Learning Platform (e.g. Class Dojo)
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video

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, e.g divorce of parents, custody issues, etc. Parents/ carers may withdraw permission, in writing, at any time.

Pupils' surnames will not be published by the school alongside their image and vice versa. Local press may insist on publishing photographs with full details of children. Permission for the press to publish these photographs must come from parents at all times. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published. Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Webcams and CCTV

The school uses CCTV for security and safety. The only people with access to this are the Headteacher and nominated office/site staff. Notification of CCTV use is displayed at the front of the school.

We do not use publicly accessible webcams in school.

12. Records, monitoring and misuse

We recognise the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to pupils and staff are minimised.

All breaches of this policy, for example receiving an offensive, abusive or inappropriate message or accessing upsetting or abuse material, must be reported and all reported incidents will be logged on 'My Concern'. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported.

The school supports pupils and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or

civil proceedings. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSL will refer details to social care or the Police.

13. Equal opportunities

Ellwood Community Primary School, strives to ensure that the culture and ethos of the school are such that, whatever the heritage and origins, abilities and needs of members of the school community, everyone is equally valued and treats one another with respect. All pupils have the right to be given opportunities and access to the full curriculum regardless of ethnicity, gender, social circumstances, ability, disability, age, nationality or citizenship. Pupils should be provided with the opportunity to experience, understand and celebrate diversity.

Inclusion

Ellwood Community Primary School, provides effective learning opportunities for all pupils. When planning, teachers set high expectations and provide opportunities for all pupils to achieve. All teachers are aware that pupils bring to school different experiences, interests and strengths, which will influence the way they learn. Teachers plan their approach to teaching and learning so that all pupils can take part in lessons fully and effectively. Specific action is taken to enable the effective participation of pupils with disabilities.

Pupils with additional needs

We endeavour to create a consistent message with parents for all pupils and this in turn should aid the establishment and future development of the School's E-Safety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of E-Safety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of E-Safety. Internet activities are planned and well-managed for these children and young people.

14. Cyberbullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the **repetitive**, **intentional** harming of one person or group by another person or group, where the relationship involves an **imbalance** of power. (See also the school behaviour policy /Anti-bullying policy).

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class. External visitors may also deliver sessions on cyber bullying.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Life Skill lessons, and other subjects where appropriate.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

15. Parental involvement

At Ellwood Community Primary School, we work closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. We believe that the support of parents/ carers is essential to implement the E-Safety policy effectively and help keep children safe. It is important that parents/carers understand the crucial role they play in this process. We aim to regularly consult and discuss E-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 E-Safety policy by informing the Headteacher or E-Safety lead.
- Parents/carers are asked on an annual basis to read through and co-sign acceptable use agreements with their children, this is completed in line with National Online Safety Day.
- 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).
- The school disseminates information to parents relating to E-Safety where appropriate in the form of: information and celebration evenings; posters; website/ learning platform postings; newsletter items; emails

Governors

We have a governor who is linked to computing throughout the school. Their role includes:

- liaising with the school regarding current practice in classrooms
- keeping up-to-date with online safety practices
- providing feedback to the Governing Body

The computing governor will be supplied with all the appropriate information on matters regarding online safety through meetings with the computing subject leader and through governors' meetings.

Monitoring and Review

The Governing Body will review this policy annually and assess its implementation and effectiveness.

Review: July 2023	By: Miss Hek and Mrs Milford	Signed: Miss Hek and Mrs Milford
Due to be Reviewed: July 2024		