ENGLEFIELD CE PRIMARY SCHOOL

POLICY AND PROCEDURES FOR E-SAFETY

Sowing the seeds for a flourishing future

Management of policy

School: This policy is implemented and managed by the Headteacher and all school teaching staff.

Governing Body: The Governing Body (led by the Development Committee) will monitor, review and update tis policy.

Approved: **Autumn 2023**

Next review: **Autumn 2025**

Associated Policies:

Positive Behaviour for Learning, Anti-Bullying, PSHE and Child Protection

Introduction & Purpose

Whether on a computer at school, a laptop at home, a games console or mobile phone, children are increasingly accessing the internet whenever they can and wherever they are. In many ways, this interaction with technology enables our children to flourish, however the potential that technology has to impact on the lives of all people increases year on year. This will undoubtedly continue and it is important that our children's education reflects this and prepares them for work and life in our digital world.

The purpose of this policy is to:

- Establish the ground rules we have in school for using the internet
- Describe how these fit into the wider context of our behaviour and PSHE policies
- How we will seek to keep our pupils safe with technology while they are in school.

Ultimately the responsibility for setting and conveying the standards that children are expected to follow when using media and information resources is one the school shares with parents and guardians. Children are often more at risk when using technology at home (where we have no control over the technical structures put in place to keep them safe). Managing screen time at home is a balancing act for parents, particularly as children grow up and become more independent; there are many points of view on what is an appropriate length of screen time, we would say that as a general guide it should be no more than 2 hours for a child in Year 6. This policy aims to set out how we educate children of the potential risks and how we attempt to inform those people who work with our children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

Organisation and Responsibilities

All staff have a responsibility to ensure that they are making appropriate use of ICT in their own teaching. One member of staff is designated Computing Subject Leader and has overall responsibility for implementing and monitoring this policy.

Digital communications with pupils and parents (email / website / Class Dojo / voice / telephone) should always be on a professional level and only carried out using official school systems.

As part of including the pupil voice in the development of our policies, like other aspects of the school and its curriculum, ICT will be included on the agendas for our School Council.

The e-Safety Subject Leader

The e-safety Subject Leader is accountable to the head teacher and governors for the day to day issues relating to e-safety. The subject leader:

- leads discussions on e-safety with the School Council
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident

- provides training and advice for staff
- meets with the Safeguarding Governor to discuss current issues and review incident logs
- reports as necessary to the Senior Leadership Team
- has responsibility for blocking / unblocking internet sites in the school's filtering system
- reviews the weekly monitoring reports from Securly

The Headteacher
The head teacher has overall responsibility for ensuring the safety of members of the school community. The head teacher and other members of the Senior Leadership Team must be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff (see flow chart on dealing with e-safety incidents)

Classroom based staff
Teaching and support staff are responsible for ensuring that they:

- maintain an up to date awareness of e-safety matters and of the school's e-safety policy and practices
- have read, understood and signed the school's Code of Conduct for staff
- report any suspected misuse or problem to the e-safety coordinator
- embed e-safety issues into the curriculum and other school activities.

What are the potential dangers?

The internet is an extremely rich resource both for learning and for recreation. All children should have access to both the internet and to email facilities as part of the school curriculum.

Usually the resources used by pupils in school are carefully chosen by the teacher and determined by curriculum policies. Use of the internet, by its nature, will provide access to information which has not necessarily been selected by the teacher. Whilst pupils will often be directed to sites which provide reviewed and evaluated sources, at times they will be able to move beyond these to sites unfamiliar to the teacher.

We will encourage children and staff to make effective use of the rich information resources available on the internet both for study and for recreation.

Initially pupils may be restricted to sites that have been reviewed and selected for content. As pupils gain experience, they will be taught how to use searching techniques to locate specific information for themselves. The school will encourage children to develop the appropriate skills and understandings that will enable them to use these resources well and safely and develop the ability to analyse and evaluate the resources they find. These skills will be fundamental in the society our pupils will be entering

The school will try whenever possible to prevent access to any materials on the Internet which may be illegal, defamatory, obscene, offensive or age inappropriate. The school's internet access will be through a recognised educational service provider, offering a filtered service. Children will normally only be allowed to use the internet when there is a responsible adult present to supervise. However, it is unrealistic to suppose that the teacher's attention will always be directed towards the computer screen. In order to minimise any instances of children accessing undesirable material members of staff will be

aware of the potential for misuse and will be responsible for explaining to pupils the expectations we have of them.

While developing technology brings many amazing opportunities, it also brings risks and potential dangers. Here are just a few examples of how easy and unfiltered access to the internet can potentially affect your child:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on social and emotional development and learning.

How we stay safe when we use ICT at our school

These are the guidelines that we recommend all our school community use in order to protect their own personal safety, the safety of others and the safety of the school.

1. Use of hand-held technology (personal phones and hand held devices)

We recognise that the area of mobile technology is rapidly advancing and we will review our stance on such technology on a regular basis.

Staff

- Members of staff are permitted to bring their personal mobile devices into school. They are required to use their own professional judgement as to when it is appropriate to use them. Broadly speaking this is that personal hand held devices will only be used in lesson time in an emergency or extreme circumstances
- Members of staff are free to use these devices in school, outside teaching time.

Pupils

- Pupils are not currently permitted to bring their personal hand-held devices into school, apart from the last day of Year 6 when their use is regulated by the class teacher.

2. Use of digital and video images

Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. 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.

When attending multi-school events, these are by nature beyond the school's control and we cannot guarantee that our pupils will not be photographed.

Our policy is:

- When taking digital / video images staff must ensure that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute;
- Digital / video images must be taken on school cameras whenever possible. When this is not possible, any photographs that staff take on personal equipment (mobile phones, tablets, must be transferred to the school's internal storage systems and must be deleted from personal equipment within 24 hours;
- Pupils and their families must not take, use, share, publish or distribute images of others without their permission;
- When signing authorisation slips for pupils to take part in multi-school events, parents acknowledge that photographs may be taken – this is something the school has no direct control of.

3. Use of the school's website

The school maintains a public facing website and all staff and children are encouraged to be involved in its construction and maintenance. Our website contains information that will be of interest to a wide audience in accordance with the school's publication scheme under the Freedom of Information Act. The website will also contain an area for the display of pupils' work. No information will be included that could identify individual children. Our school uses the public facing website for sharing information with the community beyond our school. This includes, from time-to-time celebrating work and achievements of children.

All users are required to consider good practice when publishing content.

- Personal information will not be posted on the school website
- Only pupils' first names are used on the website, and only then when really necessary.
- Detailed calendars are not published on the school website.
- Photographs published on the website or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images
- Pupils' full names will not be used anywhere on a website or blog, and never in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

4. Filtering of internet content

Content filtering provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. ***The filtering system cannot, however, provide a 100% guarantee that it will do so***. It is therefore important that the school has a policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Bradfield College ICT Department manages our internet filtering service (Securly), which allows some flexibility for changes at local level.

(i) Responsibilities

The day-to-day responsibility for the management of the school's filtering policy is held by the e-safety subject leader (with ultimate responsibility resting with the headteacher and governors).

Teaching staff have the responsibility to only set research tasks which are appropriate and, when necessary, to limit the sites pupils use for their research.

Pupil users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Teaching staff have access to sites such as You Tube on their own logins as these may be useful for lessons. Resources accessed on these sites must be prepared before the lesson so no unplanned material is viewed.

(ii) Education / training / awareness

Pupils are made aware of the importance of filtering systems through the school's e-safety education programme.

Staff users will be made aware of the filtering systems through briefings in staff meetings, training days, memos etc. (from time to time and on-going).

Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through safety awareness sessions / newsletter etc.

(iii) Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment through a weekly report from Securly.

5. e-Safety Education

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 e-Safety is therefore an essential part of the school's safety provision. Children and young people need the help and support of the school to recognise and avoid e-Safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

(i) Information literacy

Pupils should be taught in lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information by employing techniques such as:

- Checking the likely validity of the URL (web address)
- Cross checking references (can they find the same information on other sites)
- Checking the pedigree of the compilers / owners of the website

Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Pupils are taught how to make best use of internet search engines to arrive at the information they require.

e-Safety education will be provided in a number of ways:

- A planned e-Safety programme as part of Computing, PHSE and other lessons – this will cover both the use of ICT and new technologies in school and outside school

- We use the resources on Purple Mash and on CEOP's (Child Exploitation & Online Protection Centre) 'Think U Know' website as a basis for our e-Safety education http://www.thinkuknow.co.uk/teachers/resources/

- Key e-safety messages should be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises.

- Pupils should be helped to understand and adopt safe and responsible use of ICT both within and outside school.

- 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, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

(ii) The contribution of pupils to e-learning strategy

It is our general school policy to require children to play a leading role in shaping the way our school operates and this is very much the case with our e-learning strategy. Children often use technology out of school in ways that we do not in school and members of staff are always keen to hear of children's experiences and how they feel the technology, especially rapidly developing technology (such as mobile devices) could be helpful in their learning.

6. Training

It is essential that all involved in delivering and accessing learning via ICT are equipped with the knowledge of how to keep safe in order to help them understand their responsibilities. As a school community we will aim to offer regular training, as follows:

Staff

- A planned programme of formal e-safety training will be made available to staff. An audit of the safety training needs of all staff will be carried out regularly.
- It is expected that some staff will identify e-safety as a training need within the performance management process.
- The e-safety subject leader will provide advice, guidance and training as required to individuals as required on an on-going basis.

Governors
Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any subcommittee or group involved in ICT, e-safety, health and safety or safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority (Governor Services or online gel training), National Governors Association or other bodies.
- Participation in school training / information sessions for staff/parents/governors

Parents/carers
Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site.
- Parents evenings
- Reference to the parents materials on the Think U Know website (www.thinkuknow.co.uk) or others

Wider school community
School information on media literacy and e-safety sessions are open to all members of the school community in order that families and children can together gain a better understanding of these issues. The school's message is that everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

7. Professional standards for staff communication

In all aspects of their work in our school teachers abide by the Teachers' Standards as described by the DfE:

http://media.education.gov.uk/assets/files/pdf/t/teachers%20standards.pdf.

Teachers translate these standards appropriately for all matters relating to e-safety. Any digital communication between staff and pupils or parents / carers (email, chat, Class Dojo, website 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 public chat / social networking technology must not be used for these communications.

- Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice. The views and experiences of pupils are used to inform this process also.

Acceptable Use of the Internet

There are a multitude of activities that are not only inappropriate for use in a school context but are also illegal, and our Acceptable Use policy aims to ensure that users do not engage in these activities when using school equipment or systems in or out of school. Examples of inappropriate or illegal activities are listed below (**illegal are highlighted in bold**).

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- **child sexual abuse images (illegal - The Protection of Children Act 1978)**
- **grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)**
- pornography and/or the **possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)**
- **criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)**
- **promotion of any kind of discrimination**
- **promotion of racial or religious hatred**
- **threatening behaviour, including promotion of physical violence or mental harm**
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

In addition the following activities are also considered unacceptable on ICT equipment provided by the school:

- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by West Berkshire County Council and / or the school, unless by a teacher using the staff proxy to access an acceptable resource for a specific lesson
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Downloading / uploading files that causes network congestion and hinders others in their use of the internet
- On-line gambling and non-educational gaming

Use of personal social networking sites for non-educational purposes

The school has Codes of Conduct for staff and governors and Home/School Agreements with parents and pupils (refreshed annually) that recommend a common sense approach is applied to the use of social networking sites. If members of the school community suspect that misuse might have taken place, but that the misuse is not illegal (see above) it is essential that correct procedures are used to

investigate, preserve evidence and protect those carrying out the investigation. Any incidents of misuse are dealt with either through the school's disciplinary procedures or in the case of illegal activities, through the police.

By signing our Codes of Conduct and Home/School Agreements, members of the school community are agreeing to use technology in a responsible way, not only at school but also at home. Our school `rules' are:

For the safety of the whole school community:

- I will keep my password safe and will not use anyone else's (even with their permission)
- I will keep my own personal information safe as well as that of others.
- I will not interfere with the way that others use their technology.
- I will be polite and responsible when I communicate with others,
- I will not take or share images of anyone without their permission.
- I will not try to access anything illegal.
- I will not download anything that I do not have the right to use.
- I will only use my own personal ICT equipment if I have permission and then I will use it within the agreed rules.
- I will not deliberately bypass any systems designed to keep the school safe (such as filtering of the internet).
- I will not attempt to install programmes on ICT devices belonging to the school unless I have permission.
- I understand that I am responsible for my actions and the consequences
- I will tell a responsible person if I find any damage or faults with school equipment, however this may have happened.

Commitment of pupils

- I will ask an adult if I want to use the computer
- I will only use activities that an adult says are OK.
- I will take care of the computer and other equipment.
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
- I will tell an 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.
- I understand that my use of technology (especially when I use the internet) will, wherever possible be supervised and monitored.

Commitment of parents/carers

- My child will be a responsible user and stay safe while using ICT (especially the internet).
- I am aware of the importance of e-safety and will be involved in the education and guidance of my child with regard to their on-line behaviour.
- I give permission for my son / daughter to have access to the internet and to ICT systems at school.
- I know that my son / daughter has signed the Home/School Agreement and will take part in safety education to help them understand the importance of safe use of ICT – both in and out of school.
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems.

- I understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- I understand that my son's / daughter's activity on the school's ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.
- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Commitment of Staff, Governors and Voluntary Helpers

- I will be professional in my communications and actions when using school ICT systems
- I will not use aggressive or inappropriate language, I appreciate that others may have different opinions
- I understand that Codes of Conduct also apply to use of school ICT systems (laptops, email, Class Dojo, website etc.) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school
- I will not disclose my username or password, nor will I try to use anyone else's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will ensure that the taking and / or publishing of images of others is in accordance with the school's policy on the use of digital images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I will comply with the school's policy on Data Security
- I will not use personal email addresses on the school ICT systems except in an emergency
- I will not try to upload, download or access any materials which are illegal
- I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work. Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that this Acceptable Use policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school

and my use of personal equipment in school or in situations related to my employment by the school.

How the school will review any e-Safety incidents

The school needs to manage incidents that involve the use of online services with a safe and secure approach. Incidents might typically include cyber-bullying, harassment, anti-social behaviour and deception. These may appear in emails, texts, social networking sites, messaging sites, gaming sites or blogs etc. If it is suspected that the web site(s) concerned may contain child abuse images, we will report these immediately to the police.

1. More than one member of the Senior Leadership Team will be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
2. Any investigation will be carried out confidentially and will not be accessed by pupils
3. If it is necessary to visit a site or content on a computer this will be done on an office computer (i.e. one not accessible through the curriculum) and will be closely monitored and recorded to provide further protection.
4. The URL of any site containing the alleged misuse will be recorded and a note kept of 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 the incident has been fully investigated the SLT will judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisation (as relevant).
- 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
- the sending of obscene materials to a child

It is important that all of the above steps are taken as they will provide an evidence trail for the Senior Leadership Team and if necessary the governing body's Complaints, Appeals & Disciplinary Committee and possibly the police, and demonstrate that visits to these sites were carried out for child protection purposes.