Eton End

Online Safety Policy (Including EYFS)

ETON END SCHOOL
35 Eton Road, Datchet

Online Safety Policy (Including EYFS)

Relevant Statutory Regulations:	ISSR Part 3, para 7 EYFS Framework 2025 Keeping Children Safe in Education 2025 Working Together to Safeguard Children 2023 Teaching online Safety in Schools Preventing and tackling bullying Cyber bullying: advice for Heads and school staff Eton End RHSE Policy Searching, screening and confiscation Education Act 2011 Equality Act 2010 Online Safety Act 2023
Nominated members of SLT responsible for the policy:	Zoe Logan and Raheema Makhani
Updated:	1st September 2025
Date of next review:	1st September 2027

Contents

Rationale

ICT, digital and mobile technology resources are now regarded as essential to support learning, teaching and personal and social development; they form part of an essential life skill. Internet technology helps pupils learn creatively and effectively and encourages collaborative learning and the sharing of good practice amongst all school stakeholders. The Online Safety policy encourages appropriate and safe conduct and behaviour when achieving this.

This policy sets out guidelines for all members of the Eton End community who have access to and are users of school ICT systems, both in and out of the school. Users may include pupils, staff, parents, governors, Friends of Eton End, visitors and volunteers.

The Education and Inspections Act 2006 empowers Heads to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.
The school will deal with such incidents within this policy and associated behaviour, anti-bullying and safeguarding, (including PREVENT) policies and will, where known, inform parents of incidents of inappropriate online safety behaviour that effects pupils but take place out of school.

These agreements and their implementation will promote positive behaviour which can transfer directly into each pupil's life and prepare them for experiences and expectations in the ongoing stages of their lives, including the workplace. The policy is not designed to be a blacklist of prohibited activities, but instead a list of areas to discuss, teach and inform, to develop positive behaviour and knowledge leading to a safer internet usage and year on year improvement and measurable impact on online safety. It is intended that the positive effects of the policy will be seen online and offline; in school and at home; and ultimately beyond school and into the workplace.
An effective approach to online safety enables us to protect and educate the whole school in their use of technology and establishes mechanisms to identify, intervene and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but it can be categorized into four areas of risk:

Content – being exposed to illegal, inappropriate or harmful material, including extremism opinion.

Contact – being subjected to harmful online interaction with other users.

Conduct – personal online behaviour that increases the likelihood of or causes harm.

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

The policy relates to the use of technology including:

- the internet
- email
- mobile phones and smartphones
- smartwatches
- computers–desktops, laptops and iPads
- social networking
- instant messaging, chat rooms
- webcams, video hosting sites (such as YouTube)
- Promethean boards, other interactive white boards and screens
- other photographic or electronic equipment including toys.

It applies to the use of technology on school premises and educational visits and also any use, whether on or off school premises, which affect the welfare of other pupils or where the culture or reputation of the school are put at risk.

Aims

Internet use is part of the statutory curriculum and a necessary learning tool for staff and pupils. The policy demonstrates good and safe internet practice for staff and pupils; the internet and online technology provides new opportunities for young people's learning and growth, but it can also expose them to new types of risks. The aims of this policy are to allow the Eton End community:

- to use high-quality internet access safely and responsibly
- to safeguard and promote the welfare of pupils by preventing cyberbullying and other forms of abuse
- to foster an open environment in which pupils are encouraged to ask any questions and participate in an ongoing conversation about the benefits and dangers of the online world.

Curriculum and Teaching

The following subjects have the clearest online safety links (see relevant roles under Key Responsibilities):

- PSHE
- RHE
- Digital

However, as stated in the role descriptors below, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom

and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

Whenever overseeing the use of technology (devices, the internet, remote learning, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites.

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, remote learning, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g., fake news, conspiracy theories), age-appropriate materials and signposting, and legal issues such as copyright and data law.

We recognise that online safety and broader digital resilience must be a thread throughout the curriculum.

The Digital curriculum takes aspects from the 'Primary teach computing curriculum' from the STEM learning website and National Centre for Computing Education website. It includes unit topics with an overview and individual lesson plans and resources from Kapow.

https://teachcomputing.org/curriculum

Online Safety is taught as a unit with a series of lessons covering all aspects of Online Safety including cyberbullying, digital footprint, copyright, plagiarism, spam, phishing, safe searching online, media use, email, online communication, disinformation, misinformation, and conspiracy theory reviewing the Zip it! Lock it! Flag It! screensaver, watching informative videos and discussing scenarios, creating creative publications, question and answer opportunities. If websites are used in lessons, every effort is made to make sure they are secure.

Digital Prefect (s) from Y6 is/are nominated alongside digital ambassadors from Y1 upwards to work with the Director of Digital Strategy and Innovation to keep up to date with what the pupils online digital world looks like.

Key Responsibilities

The governing board (ILG) has overall responsibility for monitoring this policy and holding the Head to account for its implementation.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;

- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The Head

The Head is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) [and DDSLs are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

Supporting the Head in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

Working with the Head and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly

Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks

Working with the ICT manager to make sure the appropriate systems and processes are in place

Working with the Head, ICT manager and other staff, as necessary, to address any online safety issues or incidents

Managing all online safety issues and incidents in line with the school's child protection policy

Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy

Updating and delivering staff training on online safety

Liaising with other agencies and/or external services if necessary

Providing regular reports on online safety in school to the Head and/or governing board

Undertaking annual risk assessments that consider and reflect the risks children face

Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

Director of Digital Strategy and Innovation

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Digital curriculum in accordance with the national curriculum
- Work closely with the Eton End Safeguarding Team and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Work with parents regarding 1:1 devices.
- Liaise with the DSL & IT support regarding filtering and monitoring arrangements
- Oversees the daily online safety checks across the school:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE/ RHSE curriculum, complementing the existing computing curriculum – and how to use technology safely, responsibly and respectfully. Lessons will also cover how to keep personal information private, and help young people navigate the virtual world, challenge harmful content and balance online and offline worlds.
- Work closely with the Eton End Safeguarding Team and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE and RHSE.
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements, including remote learning agreements.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing to the Director of Digital Strategy and Innovation.
- Following the correct procedures by agreement of the Head if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Parents

Parents/carers are expected to:

- Notify a member of staff or the Head of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre https://saferinternet.org.uk/guide-and-resource/parents-and-carers
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

External Users:

External users with significant access to school systems including sensitive information or information held securely under the Data Protection Act should be DBS checked. This includes The Friends of Eton End and external contractors who might maintain the school domain name, web hosting and educational resources, which are fully GDPR compliant – which would facilitate access to cloud file storage, website documents, and email.

- Guest internet is available
- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school
- Support the school in promoting online safety and data protection
- Model safe, responsible, respectful, and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents.

Networking support:

- As listed in the 'all teaching staff' section, plus:
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant

- Work closely with the Director of Digital Strategy and Innovation to ensure that school systems and networks reflect school policy
- 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
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by SLT, including the Eton End Safeguarding Team
- 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
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy

Pupils:

- they will be educated in the safe use of the internet
- they will be responsible for using the school digital technology systems in accordance with Pupil Acceptable Use Policy
- pupils are expected to sign the Acceptable Use Policy to indicate agreement, and have their parents also sign on their behalf. They sign the age-appropriate agreement at the beginning of their school life and at the beginning of each academic year via an online form.
- Y3-Y6 will adhere to the 1:1 device policy
- they will be expected to use Atom Learning, Microsoft Teams and any other online learning platform responsibly and appropriately
- they will have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they will 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
- they will be taught to adjust their behaviours in order to reduce risks and build resilience, including to radicalisation, with particular attention to the safe use of electronic equipment and the internet.

- They will be taught to understand the risks posed by adults or young people, who use the internet and social media to bully, groom, abuse or radicalise other people, especially children, young people and vulnerable adults.
- Internet safety is integral to the school's Digital curriculum and is embedded in the teaching of PSHE and PSED. There are two special Online Safety days a year.

Inappropriate pupil behaviour:

Bullying of another person will be treated with the highest severity.

Online, Cyber Bullying

- Lessons concerning cyber bullying to be carried out termly through the Digital and PSHE curriculum
- By cyber bullying, the School is referring to: bullying by email, messages, images, calls or other electronic communication
- Use of mobile phone cameras to cause distress, fear or humiliation
- Posting threatening, abusive, defamatory or humiliating material on websites (including social networking sites)
- Hijacking or hacking email accounts
- Making threatening, abusive, defamatory or humiliating remarks in chat rooms or on instant messaging services
- The use of social media for the use of bullying, grooming, abuse and radicalisation
- Pupils should be aware that cyber bullying is generally criminal in character and that English law does apply. The School will endeavour to resolve all matters using the School's Behaviour Policy without Police involvement but parents of victims do have the right to seek Police intervention. This will be closely linked to the School's Anti-Bullying Policy and Safeguarding and Child Protection Policy and which can be read separately or in conjunction with this policy.

Parents

- Read, sign and promote the school's Acceptable Use Forms (AUF), and read the pupil Acceptable Use Policy (AUP) and encourage their children to follow it
- Consult with the school if they have any concerns about their children's use of technology
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff.

- Parents see Appendix 1 for list of online safety organisations and websites.

The school will take every opportunity to help parents understand these issues through PIMs, parents' evenings, newsletters, letters, website, online safety training and information about national and local online safety campaigns and literature. Parents 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 and school events
- access to parents' sections of the website
- Microsoft Teams

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the our Safeguarding and Child Protection policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Communicating information to:

Staff

- Through the Induction Procedure
- Information will be given to staff through INSET, staff meetings, Pre-Prep/Prep meetings and department meetings
- Online Safety training through online EduCare courses, Safeguarding Snapshots and INSET
- Via email if the Safeguarding team has information from other agencies to pass on

Educating Pupils about Online Safety:

Pupils will be taught to:

- Use technology safely and respectfully and responsibly, keeping personal information private
- Recognise acceptable and unacceptable behaviour

- Understand that people sometimes behave differently online, including pretending to be someone they are not
- Identify where to go for help and support when they have concerns about content or contact
- This is achieved by:
- Online rules and rights will be posted in all rooms where computers are used – this is every room due to the use of iPads. Online safety is embedded in the daily curriculum implicitly e.g., when logging on to a computer for a French lesson, pupils are reminded why a password is important, what to do if images appear.
- Online safety as a Digital teaching unit; how to judge the validity of website information, how to report cyber bullying, computer usage and the law, how to spot and remove viruses, why copyright is important.
- Online safety as a PSHE/Jigsaw teaching unit: how to deal with cyber bullying, how to report cyber bullying, the social effects of spending too much time online. Covered in Celebrating Difference and Relationship topics. (As part of the RHE curriculum)
- As part of the PSED/EAD areas of learning in the EYFS, online is talked about at an age-appropriate level
- Online safety as part of pastoral care – form time activities, assemblies, tutorial opportunities.
- Online safety events – such as Safer Internet Day and Anti-Bullying Week.
- All system users will be informed that network and Internet use is monitored.

Educating Parents about Online Safety

- The school will raise parents' awareness of internet safety via letters, emails, iSams and school website.
- If parents have any queries or concerns in relation to online safety these should be raised in the first instance with the Director of Digital Strategy and Innovation (DDSL).

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 Digital, PSHE / PSED and SMSC).

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 Eton End Safeguarding Team to contribute to the overall picture or highlight what might not yet be a problem. Staff need to be aware that children may be unaware that what they are discussing, viewing and sharing online is inappropriate and comes under the umbrella of safeguarding.

Non-teaching staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

The school's procedures for dealing with online safety are mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection policy and procedure
- Anti-Bullying policy
- 1:1 Device policy
- Behaviour policy
- Mobile Device policy
- IT Acceptable use agreement

We take all reasonable precautions to ensure online safety but recognise that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on pupils when they come into school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to The Safeguarding Team the same day. However, if urgent, the Safeguarding Team will be informed immediately.

Any concern/allegation about staff misuse is always referred directly to the Head unless the concern is about the Head in which case the complaint is referred to the Safeguarding Board level governor of ILG, Carrie Askew and / or the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

The school will actively seek support from other agencies as needed (i.e., the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online safety incidents involving their children. We will also inform the Police, where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law.

Sanctions available for pupils include

- Interview/counselling by a designated member of SLT
- Informing parents
- Removal of internet or computer access for an identified proportional amount of time
- Supervised access

Monitoring

The school reserves the right to monitor the use of the network, internet and e-mail systems. If it is discovered that any of the systems are being abused and/or that the terms of this policy are being breached, appropriate disciplinary action will be taken.

Property

Pupils and staff should treat any property belonging to the school with respect and reasonable care and report any faults or breakages to the Director of Digital Strategy and Innovation. Pupils with 1:1 devices should treat their property with respect and reasonable care and report any faults or breakages to a member of staff.

Viruses

Pupils and staff should be aware of the potential damage that can be caused by computer viruses. Pupils and staff must not download, install or run any programs or data (including computer games) or open emails from unknown or unidentifiable sources.

System Security

- All computers/ laptops are password protected. All laptops are bit locker and password protected.
- Pupils should not attempt to gain unauthorised access to anyone else's user area or to any information which they are not authorised to access.
- Do not make deliberate attempts to disrupt or damage the school network, any device attached to it, or any data stored on it or transmitted across.
- Do not alter school hardware in any way.
- Do not knowingly misuse headphones or any external devices e.g., printers, a mouse.
- Do not eat or drink while using the computer.
- All users should log out of any device properly as well as ensure the device is shutdown in order to protect user data.

Leaving workstations

If a person leaves their workstation for any period of time they should log out of their workstation or lock the screen.

INTERNET

The School recognises the benefits to using the Internet in an educational environment. The Internet facility is provided for school related activities only. The school monitors the use of the Internet using Net Support DNA.

- The school internet system has a filtering and monitoring system monitored by the Director of Digital Strategy and Innovation and DSL which monitors and filters all website access. The school uses a system called Net Support DNA which detects certain words or phrases as soon as it appears on the screen whether it has been typed or received by the user. A screen capture is taken of every incident, showing what was displayed at the time, who was involved and when the incident took place.

Any inappropriate material, whether it be sexual, violent, extremist or illegal in nature will be blocked and the System Administrator will alert the Director of Digital Strategy and Innovation to the inappropriate material being accessed.

Viewing, retrieving or downloading of any material that the school considers inappropriate will result in appropriate disciplinary action.

Email and ALL ONLINE MESSAGING

- Email is provided for school related purposes only. The school monitors the use of email and disciplinary action may be taken if inappropriate uses of personal emails are discovered.
- Email should be treated in the same way as any other form of written communication. Anything that is written in an email is treated in the same way as any form of writing. Pupils and staff should not include anything in an email that is not appropriate to be published generally. Any email message which is abusive, discriminatory on grounds of sex, race, disability, sexual orientation or religious belief, or defamatory is not permitted.

Privacy

All files and emails on the system are property of the School. As such, system administrators and staff have the right to access them if required.

Social Media

The school manages and monitors their social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

Searching Electronic Devices

Mobile Phones

Pupils

- Pupils are not permitted to bring mobile phones, smartwatches with internet connection or personally owned devices into school.
- Older pupils who have been given permission by the Head to walk to and from school must sign in their mobile phones at the school office when they arrive in the morning for safe keeping in a locked location during school hours.

- Co-parenting families that provide their child with a mobile phone must sign in their mobile phones at the School Office when they arrive in the morning for safe keeping in a locked location during school hours.
- Pupils must sign out their mobile at the end of the day just before leaving the school premises.
- If a pupil breaches the school policy, then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with school policy.

Staff

- The school accepts that employees will bring their mobile phones to work.
- Mobile phones and personally owned devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally owned mobile phones or mobile devices.
- Employees are not permitted to make/receive calls/texts during lessons or formal school time or use recording equipment on their mobile phones or personal devices to take photographs/videos of children.
- Staff use of mobile phones during the school day will normally be limited to the morning/lunch break, non-contact time and after school.
- Mobile phones should be switched off (or silent) and left in a safe place during lesson times. Staff should use phones in designated areas / empty classroom. The designated area is the Staff Room. If a private call needs to be made, then a request for a room can be made to the Head.
- Mobile phones are not permitted in areas where children are present.
- In the event that an employee has a particular reason for a specified period of time, they may request via the Head that they leave their phone on during working hours.
- If a staff member breaches the school policy, then disciplinary action may be taken as appropriate.
- Staff should ensure that their phones are protected with PIN/access codes in case of loss or theft.
- Mobile phones should not be used in a space where children are present unless the School phone is being used for a medical reason / approved social media, emergency on an educational visit or the teacher is in a remote location.

Staff – School Devices

- Staff are allocated school devices to use within the classroom, grounds and on educational visits
- Staff are responsible for uploading photographs and videos to the Media drive

- Staff are responsible for checking the 'Permission to be in Photographs' document issued by office staff before using images on Twitter or in the Newsletter, for example
- Staff are responsible for the content of the Tweets they post and should always ask a colleague to check the text and photographs for spelling, grammar and children included.

Photography / Images

The word photography is used in this policy to include traditional photographs and digital images of any kind, still or moving.

It is our intention to provide an environment in which children, parents and staff are safe from images being recorded and inappropriately used.

Photography and video are familiar features of life, playing a significant role in commerce, entertainment and communication; it is commonplace in our homes and it is an important element of school life.

We feel it is vital that achievements are recognised and that pupils feel valued, proud and happy. Photography is a useful tool within school and it is employed routinely in many ways, for example, record keeping, displays, special events, teachers' lessons and the children's own work.

On occasions photos are also used for the Press, school website, Twitter and other promotional purposes.

Children will only be named in photographs that are displayed within the school. We will not provide children's full names for any other purpose unless special parental consent has been received.

We are, however, sensitive to the wishes and rights of parents who may not wish their children to be photographed and who may have concerns about the use of such images.

Taking Photographs and Video

All parents are asked to give consent for photography of their child by completing a permission slip that is held on file. A register is kept of children who must not be included in press, website or any other photographic image, still or moving.

All reasonable measures will be taken to ensure that no child on the register is photographed or videoed by a visitor to school or while on an educational visit outside school. The exception to this may be photographs taken by parents at events such as concerts and church services.

From time to time, we invite the Press into school to share special events and achievements within the local community. We will allow local newspapers to take photographs of children, when appropriate, provided that parental consent has been given.

Images taken by school staff

Only the school's cameras, mobile phones and iPads are to be used by staff when taking photographs.

The printing of images is always carried out on the school premises. All photographic images held will be deleted at the end of each term.

All images taken must be deemed suitable without putting the child in any compromising positions that could cause embarrassment or distress.

Under no circumstances will an imagery equipment be allowed into the bathroom/ Y4-6 changing rooms areas unless a member of the Senior Management team is present. For example, if staff in the Early Years would like photos of the children washing their hands for hygiene posters a member of the senior leadership team must be present.

Photographs taken as records of events or for educational purposes may be displayed around the school. They are then archived or shredded after use.

Photographs used for evidence in the Early Years Learning Journeys will be transferred to the parent at the end of the Reception year.

Photographs are not exchanged with anyone outside school or removed for private use by any employee or volunteer.

Images taken by non-school staff

When a commercial photographer/filmmaker is used we will:

- Provide a clear brief
- Issue Identification
- Inform parents and children
- Obtain consent
- Not allow unsupervised access to children

Images taken by children

The school encourages children to take photographs on school trips or on residential visits using a disposable cameras / school phones / school iPads as a way of recording events.

There is no reason why pupils should not be allowed to take photographs so long as anyone photographing respects the privacy of the person being photographed. This is seen as part of the school's code of behaviour.

Infringement of this respect of privacy is akin to bullying and will be dealt with in the same way as any other breach of school discipline.

Under no circumstances will pupils be allowed to bring to school or take on trips any electronic devices such as tablets, smartphones, expensive smartwatches, laptop or other computer devices which have the capability to film videos or internet access.

Should the school learn about any inappropriateness of image use involving our pupils or staff, we will immediately act and report it as we would for any other child protection issue.

This policy should be read in conjunction with all school policies, in particular:

ICT, Mobile Device, 1:1 Device, PSHE, Safeguarding, Remote learning and SMSC.

The Online Safety Policy and Acceptable Use Policy are reviewed at or prior to the start of each academic year.

Additionally, the policy will be reviewed promptly upon:

- Serious and/or frequent breaches of the acceptable internet use policy or other in the light of online safety incidents.
- New guidance by government / LA / safeguarding authorities.
- Significant changes in technology as used by the school or pupils in the wider community.
- Online safety incidents in the community or local schools which might impact on the school community.
- Advice from the Police.

Between revision of this policy and the full Governors meeting, the Chairman has

executive powers to approve the introduction of the policy.

Cyber-bullying

Definition

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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school Behaviour policy.)

Preventing and addressing cyber-bullying – Refer to the Safeguarding and Child Protection policy.

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. The Director of Digital Strategy and Innovation will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact.

The school also sends information on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices

The Head, and any member of staff authorised to do so by the Head (as set out in our Search and Confiscation policy) can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from Head.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it

- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to Head and DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our Searches and confiscation policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Eton End recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Eton End will treat any use of AI to bully pupils in line with our [anti-bullying/behaviour] policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

The curriculum includes disinformation, misinformation and conspiracy theory discussion.

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the Director of Digital Strategy and Innovation.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and DDSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

Links with other policies

APPENDIX 1 – Useful contacts/resources

Organisation/Resource	What it does/provides
Thinkuknow	NCA CEOPs advice on online safety
disrespectnobody	Home Office advice on healthy relationships, including sexting and pornography
UK safer internet centre	Contains a specialist helpline for UK schools and colleges
swgfl	Includes a template for setting out online safety policies
internet matters	Help for parents on how to keep their children safe online
parentzone	Help for parents on how to keep their children safe online
childnet cyberbullying	Guidance for schools on cyberbullying
pshe association	Guidance and useful teaching resources covering online safety issues including pornography and the sharing of sexual images
educateagainsthate	Practical advice for parents, teachers and governors on protecting children from extremism and radicalisation.
the use of social media for online radicalisation	A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
UKCCIS	The UK Council for Child Internet Safety's website provides: • Sexting advice • Online safety: Questions for Governing Bodies • Education for a connected world framework
NSPCC	NSPCC advice for schools and colleges
net-aware	NSPCC advice for parents
commonsensemedia	Independent reviews, age ratings, & other information about all types of media for children and their parents
searching screening and confiscation	Guidance to schools on searching children in schools and confiscating items such as mobile phones
lgfl	Advice and resources from the London Grid for Learning

Information and support

- There is a wealth of information available to support schools, colleges and parents to keep children safe online in KCSIE 2022, Annex C.
- You can find out more about how children use social media, the apps they use, the risks they face, how to use privacy settings, and advice and tips about how to talk to children about online safety at:

The UK Safer Internet Centre website:	http://www.saferinternet.org.uk
CEOP's Thinkuknow website:	http://www.thinkuknow.co.uk http://www.thinkyouknow.co.uk/parents
Internet Matters:	http://www.internetmatters.org
Childnet:	http://www.childnet.com/sns
NSPCC:	http://www.nspcc.org.uk/onlinesafety
Parent Zone:	http://www.parentzone.org.uk

Ask About Games (where families make sense of video games):
http://www.askaboutgames.com

APPENDIX 2 – Acceptable Use Agreements

Nursery – Nursery https://forms.office.com/e/X8Pcb9p3wY

Pre-Prep - https://forms.office.com/e/4Fu8VUEEnq

Prep - https://forms.office.com/e/WPn81ec7W8

Appendix 3 - Good Practice Guide

Staff Personal Safety

It is vitally important that staff are careful about content that they search out or download. Every time you view a page on the internet, it is possible to trace your visit back to the school computer. This means that it is possible to tell if the school computer was being used to look at inappropriate web pages. Weekly checks are made by the Deputy Head Pastoral regarding acceptable use.

Staff need to ensure that films or other material shown to children are age appropriate.

Staff must be aware of their responsibilities to the school when using social networking sites such as Facebook. Our staff code of conduct and confidentiality policy must be adhered to at all times, even outside of working hours. It is important to maintain your status as a professional teacher.

Disciplinary action could result if the school is brought into disrepute.

- Staff must not post anything on any online site that could be construed to have an adverse impact on the school's reputation.
- Staff must not post photos related to the school on any internet site including pupils, parents, staff or the school branding (uniform).
- Staff must not form online friendships with pupils and parents.
- Staff must not post anything on to social networking sites that would offend any other member of staff, pupil or parent using the school.
- Staff will be required to attend an annual internet safety course and ensure that they pass this information on to the children in their care.
- Staff should use their school email account for all school-related communications.
- Staff to be aware of the various members of staff responsible for Safeguarding issues – Zoe Logan, Deputy Head Pastoral (DSL); Rachael Cox, Head (DDSL): Sarah Bond, Deputy Head Pastoral (DDSL) and Director of Digital Strategy and Innovation (from Nov' 23 DDSL).

Pupils

Pupil Personal Safety

- The school will organise internet safety lessons on a termly basis with one from an external presenter.
- Pupils must not play with or remove any cables etc that are attached to a school computer.

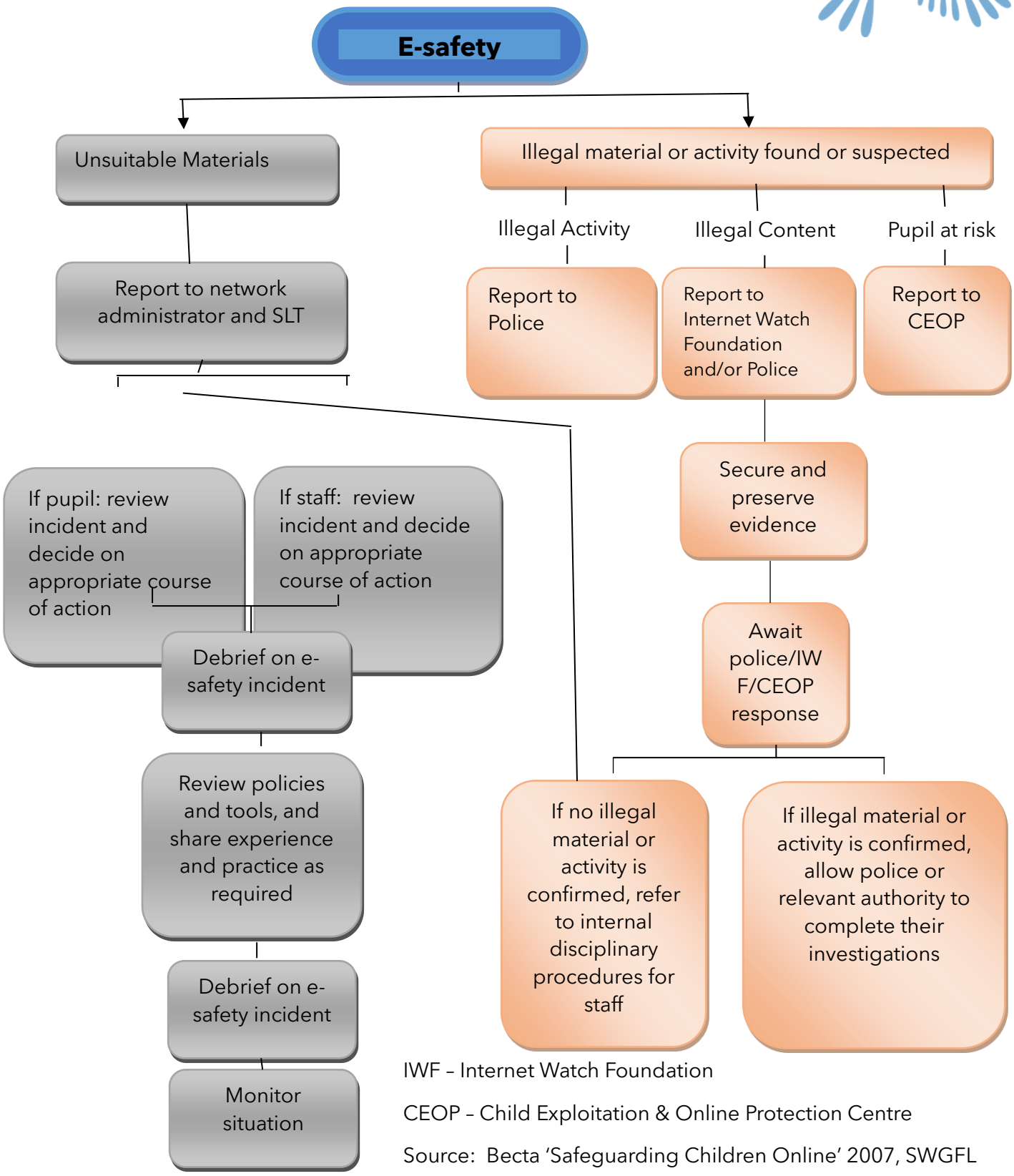
- Pupils will be taught how to stay safe when working online at school and at home.
- Pupils must not post anything on to social networking sites that would offend any other member of staff, pupil or parent using the school.
- Pupils must not post anything on any online site that can be constructed to have an adverse impact on the school's reputation.
- Pupils must not post photos of video related to the school on any internet sites including pupils, staff, parents or the school branding (uniform).
- Pupils should never reveal their full name, any address or contact details, any school or network user ID or password online, even if communicating with known acquaintances.
- Pupils should be aware that the potential exists for predators to remain entirely anonymous and easily pose as someone else.
- Pupils should employ a healthy mistrust of anyone that they "meet" online unless their identity can be verified.
- The use of chat rooms and social networking sites are not permitted in school.
- Do not arrange to meet anyone you have met on the internet - people are not always who they say they are.

Parents

- Parents will be invited to online safety events run by the Director if Digital Strategy and Innovation and/or external presenters, which will consist of advice and useful tips to help support them in ensuring their child's computer and internet safety at home.
- Parents need to be aware that parental control software is often available via their ISP so that they can manage and control their child's computer and internet activity. Mobile phone operators also offer free parental control software services to limit the kind of content your children can access through the mobile network.
- Parents need to be aware that the parental control software does not replace the need for supervision and education when working on the internet.
- Computers for children should be used in a shared space where parents can see the screen.
- Parents should take an interest in their children's internet use and discuss various issues pertaining to the internet.
- Parents should be aware of various age limits on games and social networking sites. These are there for a reason.
- Parents should discuss the care needed when their children meet online "friends". Only talk to people they know. Parents should remind their children not to give out any personal details nor details of family and friends, even to people they know.

- Parents should encourage their children to tell them if anything online makes them feel uncomfortable.
- Parents should make their child aware of the dangers of meeting someone they have only met online.
- Parents should be aware that they are in control and that they have every right to check on their children's online activities as well as their mobile usage.

Appendix 4: E-Safety Incident Flow Chart



IWF – Internet Watch Foundation

CEOP – Child Exploitation & Online Protection Centre

Source: Becta 'Safeguarding Children Online' 2007, SWGFL