Online Safety Policy

Schedule for Development, Monitoring and Review

This Online Safety Policy was approved by the school governing body on:	31.01.25
The implementation of this Online Safety Policy will be monitored by:	Head Teacher and Governors
Monitoring will take place at regular intervals:	Once a year
The governing body will receive a safeguarding report on the implementation of the Online Safety Policy on a termly basis as part of the Head Teachers report.	At Full Governing body meetings.
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	January 2026
Should serious online safety incidents take place, the following persons/agencies should be informed:	Head Teacher, DSL, Simon Brown (LA Strategic ICT Manager), Police if appropriate, LADO

Schedule for Development, Monitoring and Review	
Scope of the Online Safety Policy	
Policy Development, Monitoring and Review	
Process for Monitoring the Impact of the Online Safety Policy	
Policy Responsibilities **a. Headteacher and Leadership Team** **b. Governors** **c. Online Safety Lead** **d. DSL** **e. Curriculum Leads (If applicable)** **f. Teaching and Support Staff** **g. Network Manager and Technical Staff**	

h. Learners **i. Parents and Carers** **j. Community Users and Visitors**	
Online Safety Education Programme and Training **a. Curriculum for Pupils** **b. Contribution from Learners** **c. Staff and Volunteers** **d. Governors** **e. Families** **f. Adults and Agencies**	
Professional Standards	
Acceptable Use	
Filtering and Monitoring	
Reporting and Responding to Online Safety Issues	

This policy should be read in conjunction with the following policies

- Acceptable Use Policy
- Data Protection Policy
- Mobile Technologies Policy
- Safeguarding and Child Protection Policy
- Social Media Policy
- Technical Security Policy

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Epinay Business and Enterprise School Epinay Business and Enterprise School to safeguard members of our school community online in accordance with statutory guidance and best practice. This Online Safety Policy has been produced with reference to the statutory documents in the attached 'Legislation' Appendix.

This Online Safety Policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Epinay Business and Enterprise School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication

- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through normal communication channels such as staff meetings.
- is published on the school website via the policy page.

The DfE guidance "Keeping Children Safe in Education" states:

> **"Online safety** and the school or college's approach to it should be reflected in the child protection policy"
>
> As a result the Child Protection and Safeguarding Policy will reflect this Online Safety Policy

Policy Development, Monitoring and Review

This Online Safety Policy has been developed by the Head Teacher in conjunction with the DSL and E safety Lead Practitioner and supported by the ICT in Schools team.

Process for Monitoring the Impact of the Online Safety Policy

The impact of the Online Safety Policy and practice is regularly evaluated through

The review/audit of online safety incident logs; behaviour/safeguarding reports; staff feedback, learners' parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors using E-safety log and Cpoms
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising though regular communication, social media and workshops
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.
- logs of reported incidents from Smoothwall Monitor
- monitoring logs of internet activity (including sites visited) if possible
- internal monitoring data for network activity supplied by ICT in Schools possibly
- surveys/questionnaires of:
    - learners
    - parents and carers
    - staff.

Policy Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

(a) Headteacher and Leadership Team

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to the Online Safety Lead.
- The headteacher, DSL and the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The headteacher/senior leaders are responsible for ensuring that the Online Safety Lead, and all staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. The headteacher/senior leaders will receive regular monitoring reports from Smoothwall Monitor.

- take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns

(b) Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This review will be carried out by the full Governing board whose members will receive regular information about online safety incidents and monitoring reports.

A member of the governing body will take on the role via Safeguarding Link Governor reviews to include:

- regular meetings with the Online Safety Lead Practitioner
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- reporting to relevant governors group/meeting
- attend regular e safety training provided by eg: Safeguarding Partnership, Governor Support, ICT in Schools Team or other qualified organisations

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

(c) Online Safety Lead

The Online Safety Lead will:

- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL), where these roles are not combined

- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with teaching staff to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- receive reports of online safety incidents and create a log of incidents to inform future online safety developments
- provide (or identify sources of) training and advice for staff, governors, parents, carers, learners
- liaise with school, local authority technical staff, pastoral staff and support staff
- meet regularly with the safeguarding governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs
- attend relevant governing body meetings/groups
- report regularly to head teacher/senior leadership team.
- liaises with the local authority and relevant body.
- produce termly Headline reports highlighting e-safety work across the term.
- ensure the website is up-to-date and informative
- ensure communication and social media platforms are used to share online safety information

(d) Designated Safeguarding Lead (DSL)

The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- online bullying.

(e) Teaching Staff

Teaching staff will work with the Lead Practitioner to develop a planned and coordinated online safety education programme.

This will be provided through:

- detailed Schemes of Work
- PHSE and RSE programmes
- A mapped cross-curricular programme
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff Acceptable Use Policy (AUP)

- they immediately report any suspected misuse or problem to DSL for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners 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 lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies.
- have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.
- the online safety policy is followed

(f) Network Manager and Technical Staff

The school buys into the ICT in Schools SLA. A separate technical policy is in operation for the running of the technical elements.

Alongside this all technical staff must be aware of the school policy and abide by it as though they were a member of staff

(g) Learners

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology
- should 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.

(h) Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners' Acceptable Use Policy
- publish information about appropriate use of social media relating to posts concerning the school
- seeking their permissions concerning digital images, cloud services etc with new starters and updated annually
- parents'/carers' evenings, e-safety workshops, newsletters, website, and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school

(i) Community Users and Visitors

Community users who access school systems/website/learning platform as part of the wider school provision will be expected to read and agree to community user AUP on signing into school before being provided with access to school.

Online Safety Education Programme and Training

(a) Curriculum for Pupils

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways

- A planned online safety opportunities through the ICT SOW for all year groups matched against agreed framework and regularly taught in a variety of contexts.
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; RSE; Literacy etc
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- learners should be helped to understand the need for the learner acceptable use policy and encouraged to adopt safe and responsible use both within and outside school
- staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that learners 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 learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit
- it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need. These must be approved by the headteacher and put in writing to the ICT in Schools Team
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

(b) Contribution from Learners

The school acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- mechanisms to canvass learner feedback and opinion.
- appointment of digital leaders, ie school council representatives giving a voice for the students
- learners contribute to the online safety education programme e.g. peer education, online safety campaigns
- contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.

(c) Staff and Volunteers

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive safeguarding training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use policy. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours
- the Online Safety Lead Practitioner and Designated Safeguarding Lead will receive regular updates through attendance at external training events, (e.g. UKSIC, NOS, LA, other relevant organisations) and by reviewing guidance documents released by relevant organisations
- this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- the Online Safety Lead Practitioner will provide advice/guidance/training to individuals as required.

(d) Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:

- attendance at training provided by the local authority, NGA or other relevant organisation (e.g., SWGfL/NOS)
- participation in school training, assemblies, information sessions for staff or parents

A higher level of training will be made available to (at least) the Safeguarding Governor.

(e) Families

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

- *reg*ular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc
- the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons
- letters, newsletters, website, learning platform, social media
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant websites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers (see Appendix for further links/resources).

- Sharing good practice with other schools in clusters and or the local authority

(f) Adults and Agencies

The school will provide opportunities for local community groups and members of the wider community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- online safety messages targeted towards families and relatives.
- providing family learning courses in use of digital technologies and online safety
- the school will provide online safety information via their website and social media for the wider community

Professional Standards

There is an expectation that required professional standards will be applied to online safety as in other aspects of school life i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

Acceptable Use

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables in the Appendices to this document.

An Acceptable Use Policy is a document that outlines a school's expectations on the responsible use of technology by its users and it is more important for these to be understood and followed. In most schools they are signed or acknowledged by their staff as part of their conditions of employment. Student/Pupil Acceptable Use Agreement – to be displayed on ICT equipment and in areas within school. For Parents/Carers Consent - To be included on parent/carers school consent form and included remote learning policy. There is a range of acceptable use agreements in the appendices.

The Online Safety Policy and acceptable use policy define acceptable use at the school. The acceptable use policy will be communicated/re-enforced through:

- staff induction and handbook
- digital signage
- posters/notices around where technology is used
- communication with parents/carers
- built into education sessions
- school website
- peer support

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

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school
- any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- users should immediately report to a nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school email addresses should be used to identify members of staff and learners.

Filtering and Monitoring

The DfE guidance "Keeping Children Safe in Education" (2023) states:
"Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to…. risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. Governing bodies and proprietors should consider the number of and age range of their children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks. "

The school has a secure filtering solution in place which restricts access of its client groups. This filtering solution is:

- Administered by the ICT in Schools Team who use a default filtering policy across all Primary/Secondary Schools.
- Customisable at school level but any changes must be recorded in writing to the ICT in Schools Team.

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. Head Teacher is responsible for managing the monitoring strategy and processes.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice
- Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies including:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
- where possible, school technical staff regularly monitor and record the activity of users on the school technical systems
- use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)

Reporting and Responding to Online Safety Issues

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.

- School has an anonymous postbox where students can raise concerns confidentially.
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Lead Practitioner and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), the incident must be escalated through the agreed school safeguarding procedures.
- any concern about staff misuse will be reported to the Head Teacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
    - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
    - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
    - once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
        - internal response or discipline procedures
        - involvement by local authority
        - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g. peer support for those reporting or affected by an online safety incident
- incidents should be logged using the school e-safety log and CPoms.
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
    - staff, through regular briefings
    - learners, through assemblies/lessons
    - parents/carers, through newsletters, school social media, website
    - governors, through regular safeguarding updates
    - local authority/external agencies, as relevant (The Ofsted Review into Sexual Abuse in Schools and Colleges suggested “working closely with Local Safeguarding Partnerships in the area where the school or college is located so they are aware of the range of support available to children and young people who are victims or who perpetrate harmful sexual behaviour”

Incidents may occur inside and outside of the school (with impact on the school) which will need intervention. Detailed advice on dealing with such an incident can be found in the “Dealing with an Online Safety Incident”

Policy approved by Governors:	January 2026
Date of next review by Governors:	January 2027