SEA MILLS PRIMARY SCHOOL

Be Kind ● Be Brave ● Be your best

Online Safety Policy

Reviewed and approved by:	Standards Committee
Date approved:	22nd November 2023
Date of next review:	November 2024

Equality Impact assessment (EIA) Part 1: EIA Screening

Policies, Procedures or Practices		Date	
EIA CARRIED OUT BY:	Andrew Kinnear	EIA APPROVED BY:	6.11.23

Groups that may be affected:

Are there any concerns that the policy could have a different impact on any of the following groups? (please tick the relevant boxes)	Existing or potential adverse impact	Existing or potential for positive impact
Age (young people, the elderly: issues surrounding protection and welfare, recruitment, training, pay, promotion)		x
Disability (physical and mental disability, learning difficulties; issues surrounding access to buildings, curriculum and communication)		x
Gender Reassignment (transsexual)		x
Marriage and civil partnership		x
Pregnancy and maternity		x
Racial Groups (consider: language, culture, ethnicity including gypsy/traveller groups and asylum seekers		x
Religion or belief (practices of worship, religious or cultural observance, including non-belief)		x
Gender (male, female)		x
Sexual orientation (gay, lesbian, bisexual; actual or perceived)		x

Any adverse impacts are explored in a Full Impact Assessment.

Related policies and procedures

This policy statement should be read alongside our policies and procedures, including:

- Child protection
- Procedures for responding to concerns about a child or young person's wellbeing
- Dealing with allegations of abuse made against a child or young person
- Managing allegations against staff and volunteers
- Code of conduct for staff and volunteers
- Anti-bullying policy and procedures
- Photography and image sharing guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

Role and Responsibilities

The following section outlines the online and e-safety roles and responsibilities of individuals and groups within the school:

Governors

- Governors are responsible for the approval of the Online and e-safety Safety Policy and for reviewing the effectiveness of the policy. The Governors receiving regular information from the Online and E-Safety coordinator about online safety incidents.
- All governors and trustees should receive appropriate online safety information/training as part of their safeguarding and child protection training; this should be received as part of their induction and be regularly updated. It should include a focus on filtering and monitoring procedures within the school.
- Governors/trustees should ensure that the school/college leadership team and relevant staff have an awareness and understanding of the appropriate filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified.

Headteacher

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online and e-safety Co-ordinator.

- The Headteacher is responsible for ensuring that the Online and e-safety Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant. Online Safety BOOST includes access to unlimited online webinar training – further details are at https://boost.swgfl.org.uk/
- The Headteacher 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 (e.g. swgfl 360 toolkit). This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online and e-safety Co-ordinator.

Designated Safeguard Lead

- As online safety is identified as a safeguarding issue, the ultimate responsibility falls within the remit of the Designated Safeguarding Lead (DSL). Staff with appropriate skills, interest and expertise regarding online safety (such as computing leads or technical staff) should be encouraged to help support the DSL as appropriate, for example when developing curriculum approaches or making technical decisions. However, settings must be clear that ultimate responsibility for online safety sits with the DSL.
- The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety).
- The designated safeguarding lead is responsible for ensuring that appropriate filtering and monitoring is in place and that it is reviewed regularly to ensure that it is effective.
- In addition to the formal training, the DSL's knowledge and skills should be refreshed (this might be via e-bulletins, meeting other designated safeguarding leads or simply taking time to read and digest safeguarding developments) at regular intervals, as required, and at least annually. This will allow them to understand and keep up with any developments relevant to their role so that they are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school.
- They can recognise the additional risks that children with SEN and disabilities (SEND) face online, for example, from online bullying, grooming and radicalisation and are confident they have the capability to support SEND children to stay safe online.
- DSLs should ensure all members of staff know how to respond to 'sexting' concerns appropriately. For example, are staff aware that if a child discloses they have sent or received a potentially indecent image, these images should not be look at, printed, copied or forwarded.

E-Safety Coordinator

- The e-safety coordinator is the engineering computing champion
- Takes day to day responsibility for online and 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 online/e-safety incident taking place.
- Provides training and advice for staff.
- Liaises with the Local Authority.

- Liaises with school technical staff.
- Meets regularly with Safeguarding Governor to discuss current issues, review incident logs and filtering/change control logs.
- Attends relevant meetings/Governor's committee.
- Reports regularly to Senior Leadership Team/Governors.

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online and e-safety matters and of the current school online and e-safety policy and practices. This extends to the policies and procedures with regards to child on child abuse.
- They are aware of systems within their school which support safeguarding, and these should be explained to them as part of staff induction. This should include: the safeguarding policy; the behaviour policy; the staff code of conduct; and the role of the designated safeguarding lead (including the identity of the designated safeguarding lead and any deputies).
- They report any suspected misuse or problem to the Headteacher for investigation.
- They know what to do if a child tells them they are being abused or neglected.
- They have an awareness of safeguarding issues that can put children at risk of harm.
- Behaviours linked to issues such as sexting (also known as youth produced sexual imagery) put children in danger.
- They are aware that safeguarding issues can manifest themselves via child on child abuse. This is most likely to include, but may not be limited to: bullying (including cyberbullying) and sexting.
- All digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems.
- Online and e-safety issues are embedded in all aspects of the curriculum and other activities.
- Pupils understand and follow the online, e-safety and acceptable use policies.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- In lessons, where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Pupils

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's Online and e-safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

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

    - digital and video images taken at school events
    - access to parents / carers sections of the website.

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety and e-safety is therefore an essential part of the school's e-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 may include covering relevant issues through Relationships Education and Relationships and Sex Education (also known as RSE Education), and/or where delivered, through Personal, Social, Health and Economic (PSHE) education.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The online and e-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 and e-safety curriculum should be provided as part of Computing / PSHE / other lessons and is regularly revisited.
- Key e-safety messages is reinforced as part of a planned programme of assemblies and pastoral activities.
- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Staff act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that pupils are be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff are vigilant in 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 can request that Bristol City Council (or other relevant designated person) can temporarily remove 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.

Education – parents / carers

Many parents and carers have only a limited understanding of online and e-safety risks and issues yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, website,
- Parents/Carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications

Education & Training – Staff / Volunteers

All staff receive appropriate safeguarding and child protection training which is regularly updated. In addition, all staff receive safeguarding and child protection updates (for example, via email, bulletins and staff meetings), as required, and at least annually, to provide them with relevant skills and knowledge to safeguard children effectively.

Training will be offered as follows:

- A programme of formal online and e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-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.
- All new staff receive online and e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- All staff are aware of indicators of abuse and neglect so that they are able to identify cases of children who may be in need of help or protection.
- The online and e-safety Coordinator will receive regular updates through attendance at external training events (e.g from LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This online and e-safety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.
- The online and e-safety Coordinator will provide advice/guidance/training to individuals as required.

Technical – infrastructure / equipment, filtering and monitoring

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

- School technical systems are managed in ways that ensure that the school meets recommended technical requirements.
- There are regular reviews and audits of the safety and security of school technical systems.

- Servers, wireless systems and cabling are securely located and physical access restricted.
- All users have clearly defined access rights to school technical systems and devices.
- The school business manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed. The e-safety coordinator should be informed of any reports/incidents or security breaches.
- An agreed procedure is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems. Supply teachers will have access to their own secure laptop. It is the teacher's responsibility to ensure supply teachers have access and understand the policies set out in the document.
- Personal data cannot be sent over the internet or taken off the school site unless is complies with GDPR regulations.

The web filtering system introduced in April 2016 for Bristol schools categorises websites and allows access as per each school's requirements. A default 'minimum level' of filtering is blocked for all users which includes sites that are blocked as violence and Hate & discrimination.
The school will work in partnership with parents, Bristol County Council and the SWGfL to ensure systems to protect pupils are reviewed and improved.
If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the internet Service Provider 0117 9037999 cyps.it.helpdesk@bristol.gov.uk via designated staff members. Staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/ disadvantages.

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X						Y5/6	
Use of mobile phones in lessons				X				X
Use of mobile phones in social time (staff room)		X						X
Taking photos on personal mobile phones / cameras				X				X
Use of other school mobile devices eg tablets.	X						X	
Use of personal email addresses in school, or on school network		X						X
Use of school email for personal emails				X				X
Use of messaging apps (e.g. class dojo)		X						X
Use of social media			X					X
Use of blogs (Seesaw or school website)	X					X		

When using communication technologies (Class Dojo, Purple Mash) the school considers the following as good practice:

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

- Users must immediately report, to the nominated person – in accordance with the school policy - the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students/pupils or parents/carers (email) must be professional in tone and content. These communications may

only take place on official (monitored) school systems. Personal email addresses, text messaging or social media **must not** be used for these communications.

- Pupils should be taught about online and e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Mobile Technologies

Mobile technology devices may be a school owned/provided or privately owned smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

The absolute key to considering the use of mobile technologies is that the pupils staff and wider school community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device is school owned/provided or personally owned. Therefore our mobile device procedure sits alongside a range of polices including but not limited to the Safeguarding Policy, Bullying Policy, Acceptable Use Policy, policies around theft or malicious damage and the Behaviour Policy. Teaching about the safe and appropriate use of mobile technologies is included in the online safety education programme.

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Students now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, we not only have the opportunity to deepen student learning, but they can also develop digital literacy, fluency and citizenship in students that will prepare them for the high tech world in which they will live, learn and work.

Child on child abuse

All staff recognise that children are capable of abusing their peers. All staff are be clear about the school or college's policy and procedures with regard to child on child abuse. Governing bodies and proprietors ensure that the child protection policy includes:

- Procedures to minimise the risk of child on child abuse; how allegations of child on child abuse will be recorded, investigated and dealt with;
- clear processes as to how victims, perpetrators and any other child affected by child on child abuse will be supported; a clear statement that abuse is abuse and should never be tolerated or passed off as "banter", "just having a laugh" or "part of growing up";
- recognition of the gendered nature of child on child abuse (i.e. that it is more likely that girls will be victims and boys perpetrators) but that all child on child abuse is unacceptable and will be taken seriously;
- and the different forms child on child abuse can take, such as: sexual violence and sexual harassment and sexting (also known as youth produced sexual imagery):

Sexting

Although viewed by many young people as 'normal' or 'flirting', by sending an explicit image, someone under 18 may technically be producing and distributing indecent images. They risk being prosecuted, even if the picture is taken and shared with their permission and can be at increased risk of blackmail, bullying, emotional distress and unwanted attention from sex offenders. Whilst it is usually more common with teenagers, this behaviour can impact on younger children, for example risk taking behaviour or natural curiosity; all settings therefore must consider how to respond.

DSLs should access the follow the UKCCIS sexting guidance for schools and colleges and use professional judgement when responding to sexting concerns.

If a member of staff is made aware of an incident of sexting in order to safeguard themselves, the member of staff should NOT under any circumstances view the image. The member of staff should step away from the device, ask the pupil to keep the image and contact the DSL or police immediately.

Risk assessment

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. The school takes all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Bristol County Council can accept liability for the material accessed, or any consequences of internet access.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The headteacher will ensure that the internet policy is implemented and compliance with the policy monitored.

Prevent

The Counter-Terrorism and Security Act, which came into force on 1 July 2015, requires certain authorities, including schools, to "have due regard to the need to prevent people being drawn into terrorism". This is known as the 'Prevent duty'. The duty covers all types of extremism, whether political, religious or ideological. The duty to protect pupils from the risk of radicalisation should be seen as part of schools' wider safeguarding duties, similar to the responsibility to protect pupils from harm caused by, for example, drugs, gangs, neglect or sexual exploitation.

Our school safeguarding procedures are robust and take the risk of radicalisation into account, including with regard to visiting speakers. Appropriate internet filtering systems are in place to ensure pupils are not exposed to harmful content online.

Sea Mills Primary school is a "safe space" for pupils to discuss sensitive topics, including terrorism and extremist ideas. They are taught how to recognise and manage risk, think critically and make reasoned arguments.

The government's Educate Against Hate website says that where a member of staff has a concern, he/she should follow the school's usual safeguarding procedures. Concerns should be discussed with the designated safeguarding lead, who may decide to involve other agencies such as the LA or local police.

Password Security

Policy Statements:

- These statements apply to all users.
- All school networks and systems will be protected by secure passwords.
- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the online safety group (or other group).
- All users (adults and learners) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords must not be shared with anyone.
- All users will be provided with a username and password by esafety lead

Password requirements:

- Passwords should be long. Good practice highlights that passwords over 12 characters in length are considerably more difficult to compromise than shorter passwords. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length trumps any other special requirements such as uppercase/lowercase letters, number and special characters. Passwords should be easy to remember, but difficult to guess or crack.
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school
- Passwords must not include names or any other personal information about the user that might be known by others
- Passwords must be changed on first login to the system

Learner passwords:

- Records of learner usernames and passwords for foundation phase learners can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user
- Password requirements for learners at Key Stage 2 and above should increase as learners progress through school.
- Users will be required to change their password if it is compromised.
- Learners will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.
- Suitable arrangements should be in place to provide visitors with appropriate access to systems which expires after use. *(For example, your technical team may provide pre-created user/password combinations that can be allocated to visitors, recorded in a log, and deleted from the system after use.)*
- In good practice, the account is "locked out" following six successive incorrect log-on attempts.
- Passwords shall not be displayed on screen.