ONLINE SAFETY POLICY

2024

HEADTEACHER: ALEX BRAMLEY

Last Reviewed	**December 2024**
Reviewed By (Name)	**Eleanor Swift**
Job Role	**Computing Co-Ordinator**
Next Review Date	**December 2025**

Contents

1. Introduction

1.1. **The purpose of this policy is to:**

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- provide staff and volunteers with the overarching principles that guide our approach to online safety
- ensure that, as school, we operate in line with our values and within the law in terms of how we use online devices.

1.2. **This policy should be read in conjunction with:**

- AI Policy
- Child Protection and Safeguarding Policy
- Staff ICT and Electronics Devices Policy
- Behaviour Policy
- Data Protection Policy
- Social Media Policy

1.3. We believe that use of online services and tools can provide enhanced collaborative learning opportunities, high engagement, allow access to rich and up-to-date content and can support the needs of all our pupils. We embed the use of online technologies throughout the school as part of learning and we also aim to give pupils the skills to interact with the ever-changing online world in a balanced, healthy and safe way. This is achieved through both implicit measures such as automatic filtering of content and protections in school and explicit measures including active teaching of online safety threaded though all sessions, clear rules for the use of devices and the internet by any people in school and actions to take if this is infringed.

2. Responsibilities

2.1. This Policy applies to all staff, including temporary staff, consultants, governors, volunteers, and contractors, and anyone else working on our behalf. It is also applicable to pupils, but this group will require support and guidance from staff as part of their learning.

2.2. All staff are responsible for reading and understanding this policy before going online at school.

2.3. All leaders are responsible for ensuring their staff team read and understand this policy before using going online at school and that they follow this policy, including reporting any suspected breaches of it.

2.4. There are a number of staff in the school who are key contributors to Online Safety Policy and development:

- Eleanor Swift, Computing Co-Ordinator
- Alex Bramley, Headteacher
- Emily McKinnon, Deputy Safeguarding Lead
- Sean D'Souza Walsh, Deputy Safeguarding Lead
- Our Data Protection Officer

3. Legislation

3.1. This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England. Summaries of the key legislation and guidance are available on:

- **online abuse**
- **bullying**
- **child protection**

4. Aims

4.1. We believe that children and young people should never experience abuse of any kind. Children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

4.2. The 4 C's of online safety are a framework that categorizes online risks into four areas:

- Content: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, and racist or radical and extremist views.
- Contact: Being subjected to harmful online interaction with other users, e.g. commercial advertising and adults posing as children or young adults.
- Conduct: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- Commerce: Risks such as online gambling, inappropriate advertising, phishing and financial scams.

4.3. In considering the online safety of our pupils, we have used the previous categories of risk, this policy aims to anticipate these risks and guard against them:

- To ensure that automatic protections such as filtering are in place and kept up to date with evolving risks.
- To teach a relevant, up-to-date online safety curriculum which is progressive from Early Years to the end of Year 6.
- To thread the teaching and reinforcement of online safety understanding though all subjects and embedded in the day-to-day lives of pupils and staff.
- To train staff and governors in the latest methods of enhancing the online safety of all pupils and responding to new threats to pupils' online safety.
- To communicate with pupils about their experiences, understanding and concerns through pupil voice surveys and as part of learning walks.
- To advise parents regarding protecting online content in the home and on devices used by pupils.
- To have in place, up to date acceptable use contracts for pupils, parents and staff.
- To provide clear guidance in the correct monitoring and reporting of online safety incidents.
- To have clear guidance about the steps to take in the case of incidents related to online safety.
- To have data policies outlining how we keep data secure.

5. Curriculum

5.1. Online safety is embedded throughout the curriculum however it is particularly addressed in the following subjects:

- Computing
- RSE
- PSHE
- Citizenship

The curriculum and the school's approach to online safety is developed in line with the DfE's 'Teaching online safety in school' guidance and the associated UK Council for Child and Internet safety's 'Education for a connected world framework.'

5.2. We use the Purple Mash Computing Scheme of Work Online Safety units to teach many aspects of online safety within the context of Computing as a subject. This aims to give pupils the underpinning knowledge of aspects of the online world to help them develop behaviours that can navigate safely and confidently regardless of the device platform or app they're using. It also aims to help pupils develop appropriate scepticism and reasoning when they encounter new online experiences to be able to evaluate the risks or potential pitfalls of these encounters.

We further reinforce and expand this teaching through the PSHE and RSE curricula which also cover aspects of online safety.

We supplement this teaching with whole school online safety awareness, assemblies and through role modelling in the day-to-day life of the school.

Online safety teaching is appropriate to pupils ages and developmental stages as well as being flexible enough to be tailored to any specific emerging threat within the community.

The underpinning knowledge and behaviours pupil learn through the curriculum include the following:

- Evaluating what they see online.
- Recognising techniques used for persuasion.
- Clear understanding of acceptable an unacceptable online behaviour.
- Identifying online risks.
- How to seek support.

5.3. External resources are reviewed by teachers prior to using them for the online safety curriculum to ensure that they are appropriate and to ensure that they are valid sources of information based upon evidence and of high quality. When external visitors are invited into school to deliver certain aspects of the online safety curriculum the head teacher and DSL ensure that the visitors selected are appropriate. Before conducting a lesson or activity on online safety the class teacher and DSL consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises staff members on how best to support any people who may be especially impacted by lesson or activity. Lessons and activities are planned so they do not draw attention to individual pupils who may be experiencing difficult circumstances. If a staff member is concerned about anything pupils raise, they will make a report in line with the safeguarding policy.

6. Resources

6.1. The technology resources used in school to access the internet include:

- Laptops
- iPads

6.2. The following functions are in place to protect content:

- Content filtering
- Security features such as anti-virus software and firewalls.
- Protection against unauthorized installation of software; admin management.

All websites used are evaluated by the teacher prior to classroom use.

Staff adhere to copyright laws when creating materials for use in school.

Access is only given to staff and pupils once acceptable use agreements have been signed.

Children use the Internet under supervision and with direction in school.

6.3. The headteacher and Data Protection Officer ensure that filtering is in place. Filtering is selected to be suitable for the pupils' ages, number of users on the network, not over-blocking or too restrictive. Any changes to the filtering must be authorized by the headteacher in consultation with the Data Protection Officer.

If persons including pupils deliberately breach the filtering in place, this, matter is managed though the behaviour policy (pupils) or the disciplinary policy (staff).

If any illegal material is believed to have been accessed this matter will be passed immediately to the appropriate agency e.g. CEOP or the police.

All network users have their own usernames and passwords. Users are responsible for keeping their passwords private. Staff must change passwords every six months.

Users must lock devices when unattended.

7. Inclusion

7.1. We aim to enable all pupils to have a thorough understanding of how to protect their own and others' safety online. This includes children of all abilities, social and cultural backgrounds, those with SEND and EAL speakers. We place particular emphasis on the flexibility technology brings to allowing pupils to access learning opportunities, particularly pupils with SEN and disabilities. With this in mind, we will ensure additional access to technology is provided throughout the school day and in some cases beyond the school day. The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less a comprehensive support network from family and friends in staying safe online e.g. pupils with SEND and LAC. Relevant members of staff e.g. the SENCO and designated teacher for LAC work together to ensure the curriculum is tailored so these pupils receive the support that they need.

8. Monitoring

8.1. Monitoring will be achieved through:

- Observations
- Learning walks
- Work scrutiny
- Reflective teacher feedback
- Learning environment monitoring
- Dedicated Leadership time

8.2. Evaluation and feedback will be achieved through:

- Dedicated leadership time.
- Using recognised national standards for benchmarking.
- Feedback on whole school areas of development regarding online safety given and discussed during staff training and staff meetings.

8.3. Concerns regarding a staff member's online behaviour are to be reported to the headteacher in line with the Staff code of Conduct and Disciplinary Policy.

Concerns regarding a pupil's online behaviour are to be reported to the DSL who will investigate in line with the Child protection and safeguarding and Behaviour policies with the headteacher and with the support of the IT Network manager if required.

The DSL records all online safety incidents.

9. Training

9.1. All staff receive safeguarding and child protection training which includes online safety at least annually. The DSL and deputies undergo training that is updated at least every two years. The DSL and deputies also receive regular online safety updates. All staff are informed about how to report online safety concerns in accordance with the relevant policies.