ONLINE SAFETY POLICY

REVIEWED 16th September 2024
RATIFIED 18th September 2024

REGULATIONS
PART 3: Welfare, Health and safety.
TO BE READ IN CONJUNCTION WITH:
Child Protection and Safeguarding Policy

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, **Keeping children safe in education 2024** and linked advice for schools on:

- **Teaching online safety in schools**
- **Preventing and tackling bullying** and **cyber-bullying: advice for Head of Schools and school staff**
- **Searching, screening and confiscation**

It also refers to the Department'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.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Proprietorial board

The Proprietorial board has overall responsibility for monitoring this policy and holding the Executive Team and Head of School to account for its implementation.
The Proprietorial Board will co-ordinate regular meetings with the Executive Team and Head of School to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).
All of the Proprietorial Board will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's IT systems and the internet

3.2 The Head of School

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

3.3 The designated safeguarding lead

Details of the school's DSL and deputy DSL are set out in our child protection and safeguarding policy as well relevant job descriptions.
The DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working to address any online safety issues or incidents
- 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 of School and/or critical friends.

This list is not intended to be exhaustive.

The Overarching Framework.

The schools approach to safeguarding pupils from potentially harmful and inappropriate on line material is framed around 4 x areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide,anti-Semitism, radicalisation and extremism.
- **contact:** being subjected to harmful online interaction with other users; forexample: peer to peer pressure, commercial advertising and adults posingas children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images(e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

It is recognised that an increasing number of pupils own or have access to internet enable devices and their exposure to the internet and social media platforms brings significant risks. This risk can be from people they know (including close/intimate relationships) and people they think they know but who have adopted fake profiles and are seeking to groom children for purposes of abuse and/or exploitation.
On line safety, in terms of staff awareness and educating children to remain safe whilst on-line as well as off-line, is at the core of our safeguarding commitment.
See: Useful resources below

3.3 The IT manager

The IT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's IT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.4 All staff

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 IT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use
- 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

This list is not intended to be exhaustive.

3.5 Parents

Parents are expected to:

- Notify a member of staff or the Head of School 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 IT systems and internet

Parents can seek further guidance on keeping children safe online from the following organisations and websites (see also resources section):

- What are the issues? - **UK Safer Internet Centre**
- Hot topics - **Childnet International**
- Parent factsheet - **Childnet International**

3.6 Visitors and members of the community

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

In **EYFS and Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

Pupils in **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

The safe use of social media and the internet will also be covered in other subjects where relevant.
The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our social media channel. This policy will also be available for parents on request.
Online safety will also be covered during IEP visits when appropriate.
If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head of School.
Concerns or queries about this policy can be raised with the Head of School.

6. Cyber-bullying

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

6.2 Preventing and addressing cyber-bullying

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.
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 receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training
The school also sends information/leaflets on cyber-bullying to parents so that 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 consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. This should not be done without proper consultation with the DSL.
When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the Police

Any searching of pupils will be carried out in line with the DfE's current guidance on **screening, searching and confiscation**.
Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils and staff are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.
We will monitor the websites visited by pupils and staff to ensure they comply with the above.

.

8. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use. Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. No USB devices are to be used.
If staff have any concerns over the security of their device, they must seek advice from the IT manager. Work devices must be used solely for work activities.

9. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying, the risks of online radicalisation and filtering & monitoring. 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).
The DSL 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.
More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

10. Filtering and Monitoring Systems

We actively promote monitoring at the first level within the classroom, pupils are closely supervised when accessing the internet and the carousel system of teaching ensures there are regular check-ins when working independently.

All computers with the school connect to our WAN which is provided and managed by Evolving Networks. The firewall and filtering system is a product called Fortinet and is hosted by independent school specialist MSPLab. Our school network uses Office 365 and Entra for user authentication. Microsoft Defender is present on all Windows devices which adds another layer of filtering when those devices are off-site (select staff).

Alerts and reports are in place and sent to the IT Manager who shares and meets with the Group DSL weekly to discuss and review any concerns. Biweekly meetings between the IT Manager, Group DSL and Heads of School allow feedback and updates regarding filtering issues or concerns. Any issues within the school are raised as a discussion with SLT, an incident report or a cause for concern. Termly filter tests are conducted alongside constant filter list management following any incident. Annual Filtering & Monitoring reviews are conducted by the IT Manager, Group DSL, Group Operations Manager and a member of the Proprietorial Body

Our internet filtering provider is a member of the Internet Watch Foundation (IWF), signed up to Counter-Terrorism Internet Referral Unit list (CTIRU) and blocks access to illegal content including child sexual abuse material (CSAM). A thorough annual filter test is conducted alongside constant filter list management following any incident.

Evolving Networks
https://www.evolvingnetworks.net.uk/

MSPLab
https://www.msplab.cloud/

Ninjaone RMM is used as part of the suite to provide remote access and to check logs of machines and devices on the network.

Useful Resources:

Keeping children safe in education 2024
Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk)
UK Safer Internet Centre | SWGfL
Online safety resources for schools and organisations | NSPCC Learning
https://www.childnet.com/
https://www.bullying.co.uk/cyberbullying/
https://www.ceop.police.uk/safety-centre/
https://www.gov.uk/government/publications/teaching-online-safety-in-schools