ONLINE SAFETY POLICY

INDEX

Section I: Policy

1. RATIONALE AND PRINCIPLES

a. The importance of online safety

New technology and the Internet are essential for education, business and communication in general, and the school recognises it has a duty to provide pupils with high quality resources, including Internet access, as part of their learning experience.

There are benefits to technology and the Internet but also risks and challenges:

- Children have the potential to access an enormous range of online material, some of which is not age appropriate.
- Children have the opportunity to contact and be contacted by a far wider range of people, including strangers.
- Online communication makes it harder to identify and assess the people one communicates with.
- Communication is less visible and so potentially harder to guide and supervise.

These and other factors create special risks for children.

This document sets out the school's policy for ensuring that pupils are safe at all times when using devices and communications while in school. It also indicates the measures the school will take to support parents in ensuring our pupils are safe when using devices at home.

b. Guiding principles

It is essential pupils are effectively safeguarded from potentially harmful and inappropriate online material. The school is responsible for pupils' online safety whilst they are at school. While we consider it our duty to provide reasonable guidance to families, parents must take responsibility for their children's online safety at home.
We identify four primary areas of risk:

Content
Being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide and extremism.

Contact
Being subjected to harmful online interaction with other users; for example: Peer to peer pressure, commercial advertising and adults posing as 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.

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

Our Online Safety Policy and procedures are designed to achieve effective management of these risks.

Controlling pupils' use of ICT is at best a partial solution to guaranteeing safety. We believe informing and educating students and the wider community are essential to ensuring effective online safety.

This policy addresses the particular safety issues that arise from the use of devices and the Internet. The school safeguarding applies if a child protection issue arises through online communication and the Anti-Bullying Policy applies in the case of cyber-bullying.

The school has a clear, progressive online safety education programme as part of the Computing and PSHE curriculum. This covers a range of skills and behaviours appropriate for each age group and experiences, including:

- Strategies to evaluate and verify information before accepting its accuracy
- Awareness of bias or hidden purpose
- Knowledge and skills to narrow down or refine a search
- Understanding how search engines work
- Exercising acceptable behaviour and conduct when online
- Awareness of the risks of sharing images and information online
- Awareness of what a digital footprint is and its impact on life
- Adopting a cautious approach to communicating with unknown “friends” online
- Not to download illegal files without permission (Music, Movies etc)
- Adopting strategies for identifying and reporting inappropriate materials
- Understanding the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying
- Understanding plagiarism, copyright and intellectual property
- Awareness of the risks of online gambling, in appropriate advertising campaigns and financial scams

2. MEASURES

a. Online publication of information

- The personal contact information of members of staff and students is never published on the school website or other online spaces.
- The contact details given on the school website and other online spaces are the school address, telephone number, fax number, email address and the work email addresses of members of staff.
- Students’ full names are never published online in association with their photographs.
- Parents are able to opt out of their child's photo appearing in the school's online (or offline) publications by informing the school in writing.

b. Filtering

The objective of our filtering system is to block internet access to harmful sites and inappropriate content. While no filtering system is 100% effective, our approach is to minimise risk by using effective and up to date filtering providers that ensure the system:

- Is applied to all users, school owned devices and guest devices using the school broadband connection
- Filters all internet feeds at appropriate age settings, identifies and blocks VPNs/proxy services and provides alerts when any web content is blocked
- Is able to identify the ID/IP address, time and date of attempted access and the content being blocked
- Blocks chat rooms and social networking sites except those that are part of an educational network or approved learning platform

c. **Monitoring**

The objective of our monitoring system is to allow the school to review user activity on all school devices and external devices when using the school network.
While no monitoring system can be 100% effective, our approach is to minimise risk by:

- Regular physical monitoring of screens by staff
- Ongoing network monitoring using log files of internet traffic and web access
- Ongoing individual device monitoring through software

d. Social networking

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the school's preferred system for such communications.
- The school's preferred system for social networking will be maintained in adherence with the communications policy.

School staff ensure that in their private online use:

- No reference is made to students / pupils, parents / carers or school staff
- No personal opinions are attributed to the school
- Security settings on personal social media profiles are maintained at a high level

3. PROCEDURES

Staff must be aware of their responsibilities to the school when using methods of electronic communication and social networking sites. Our confidentiality policy must be adhered to at all times, even outside working hours.

All staff should bear in mind that information that they share through internet applications, even though they are in private spaces, are still subject to copyright, data protection and freedom of information legislation, the safeguarding of vulnerable groups.

All communications with parents of current children should be made through the designated official channels.

At no time must a post be made in reference to any children, parent, staff member or other professional whom an employee comes into contact with through work.

No photographs or materials should be published identifying the setting or children.
In order to maintain professional boundaries, staff should not accept personal invitations to be friends on internet applications such as social networking sites from parents or students.
Staff must not use their mobile phones to take photos or go on social networking sites or similar whilst in the school.

Staff members are advised to set their online profiles as private so that only friends are able to see their information. This can help to prevent any accidental breaches of this policy.
Serious breach of the electronic communication policy (e.g. remarks or comments that breach confidentiality and/or are deemed to be of a detrimental nature to the school or its employees, or posting or publishing photographs of the children, setting or another staff member unless with staff permission) may be deemed gross misconduct and may result in disciplinary action in line with disciplinary procedures.

a. Guidelines in social networking practices

Staff are encouraged to use the following guidelines in social networking practices:

- Remember that no information sent over the Internet is totally secure and therefore if you do not wish for the information to become public, refrain from using a social networking site.
- Even though you may consider that you are anonymous or using an alias you may be recognised.
- Maintain professionalism, honesty and respect.

b. Students' use of personal devices

- The school discourages the use of student mobile phones in school except in particular circumstances when a parent wishes their child to have access for their own safety.
- If a student 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 the school policy.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

c. Staff training

Online safety is a key element of induction training for all new members of staff, who are required to complete annual online safety training at the beginning of the school year.

Additional staff training in safe and responsible Internet use and on the school Online Safety Policy is provided at least annually to reflect any policy changes and technological developments.

d. Educating pupils

Online safety is an important theme in assemblies, PSHE lessons and the wider curriculum. Students are taught how to use the internet and access online resources safely. Lessons ensure that students are able to recognise and report inappropriate content to a member of staff or their parents.

e. Supporting & informing parents

Parents benefit from guidance and support provided by the school:

- Online safety information is regularly provided to parents and the wider community through the newsletter and other home-school communication channels.
- Online safety talks are provided for parents at least once a year.
- In the event of inappropriate use of the Internet at home by pupils, the school will provide all reasonable assistance and support to parents to help resolve the issue.

f. Review of Systems

We ensure that our online safety systems are robust through a system of regular checks and a thorough annual review.

Checks to the filtering and monitoring systems are conducted to ensure that the system is proving as effective as possible. A record of checks is maintained that includes when each check took place, who by, what was checked and any resulting actions.

An annual review takes place as part of our self evaluation process to ensure the filtering and monitoring system is fit for purpose and achieving our objectives.

The review is conducted by the IT service provider, DSL, SLT and Designated Safeguarding Governor with recommendations to the board as part of our annual safeguarding report.
In exceptional circumstances a full review may occur more often if:

- A significant safeguarding risk is identified
- There is a significant change in working practice (e.g remote teaching and learning)
- A new technology is introduced

This policy is reviewed and updated in line with the annual review. Any significant deficiencies and weaknesses in the policy are remedied without delay with prior approval of at least one member of the Board.

g. Response to inappropriate content

If members of staff or students come across inappropriate content online, the 'Response to Inappropriate Content' guidelines are followed. Incidents are reported to the Designated Safeguarding Lead or member of the safeguarding team. The DSL will decide on the appropriate action to take.

The following are the steps to follow if a member of staff discovers inappropriate content on a computer:

1. **Cover**

Cover up the screen, move it or switch the monitor off so that pupils can no longer see the content.

2. **Evidence**

If the content is sexually explicit, note down the web address. Do not make a copy, do not take a screenshot. When you have noted the web address, close the application or turn off the computer.
If the content is not of a sexually explicit nature, take a screenshot and save it on the network in a location that cannot be accessed by pupils.

3. **Report**

Incidents involving sexually explicit or inappropriate content must be reported to the Designated Safeguarding Lead immediately. It is important to note that inappropriate content can be encountered by accident, so special care must be taken to understand the circumstances.

Section II: Roles and responsibilities

Designated Safeguarding Governor

The DSG has overall strategic responsibility for online safety including filtering and monitoring systems. They ensure that appropriate resources are made available to meet the required standards.

Designated Safeguarding Lead

The DSL takes overall responsibility for the implementation of online safety including filtering and monitoring systems. They work closely with all stakeholders to ensure that our online safety policy and procedures are robust, well communicated, implemented and reviewed regularly.

Senior Leadership Team

All members of the SLT are part of the safeguarding team and support the DSL in implementing our online safety policy and procedures. This includes:

- Procuring filtering and monitoring systems
- Documenting decisions on what is blocked or allowed and why
- Reviewing provision
- Overseeing reports
- Ensuring staff understand their role and are properly trained to follow school policies and procedures

IT Service Leader/Provider

The ITS Leader provides technical expertise that supports the work of the safeguarding team to ensure that filtering and monitoring systems are working efficiently.
This includes technical responsibility for:

- Maintaining filtering and monitoring systems
- Providing filtering and monitoring reports
- Completing actions following concerns or checks to systems

The ITS Leader works with the senior leadership team and DSL to:

- Procure systems
- Identify risk
- Carry out regular checks
- Provide reports on activity in a simple understandable format
- Report safeguarding concerns to the DSL
- Contribute to the annual review of filtering and monitoring systems

In order to fulfil this role, it is an expectation that the ITs Leader completes the appropriate safeguarding training.

All Staff

All staff are responsible for supporting online safety by:

- Providing effective supervision when students are working online
- Maintaining awareness of how devices are being used
- Supporting the implementation of the school online policy and procedures
- Modelling safe, professional and responsible online behaviour
- Reinforcing online safety guidelines that are taught in our PSHE curriculum

Staff must report concerns to the safeguarding team immediately if they:

- Witness or suspect unsuitable material has been accessed
- Can access unsuitable material
- Are teaching topics which could create unusual activity on the filtering logs
- Identify a failure in the software or abuse of the system
- Perceive unreasonable restrictions affecting teaching and learning or administration
- Notice abbreviations or misspellings that allow access to restricted material

Students

Students are expected to apply the guidelines taught in school to support their online safety.

- Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy where appropriate.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- To understand the importance of reporting abuse, misuse or access to inappropriate materials
- To know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- To know and understand school policy on the use of mobile phones, digital cameras and handheld devices.
- To know and understand school policy on the taking / use of images and on cyber-bullying.
- To understand the importance of adopting good online safety practice when using digital technologies out of school
- To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home to help the school in the creation/ review of online safety policies

Parents/carers

Parents are expected to understand and reinforce the school Online Safety Policy, taking responsibility for their children's use of the internet outside of school:

- To support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images
- To read, understand and promote the school Pupil Acceptable Use Agreement with their children
- To access all modes of digital school communication and records in accordance with the relevant school Acceptable Use Agreement.
- To consult with the school if they have any concerns about their children's use of technology

Section III: Websites for additional information regarding Online Safety

There is a wealth of information available to support schools, colleges and parents/carers to keep children safe online. The following list is not exhaustive but should provide a useful starting point:

Advice for governing bodies/proprietors and senior leaders

- Childnet provide guidance for schools on cyberbullying
- Educateagainsthate provides practical advice and support on protecting children from extremism and radicalisation
- London Grid for Learning provides advice on all aspects of a school or college's online safety arrangements and guidance on platform advice
- NSPCC provides advice on all aspects of a school or college's online safety arrangements
- South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements

Remote Education, Online Learning and Video Conferencing

- UK Safer Internet Centre provides guidance on safe remote learning

Support For Children

- Childline for free and confidential advice
- UK Safer Internet Centre to report and remove harmful online content
- CEOP for advice on making a report about online abuse

Parental Support

- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology
- Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents
- Internet Matters provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world
- Let's Talk About It provides advice for parents and carers to keep children safe from online radicalisation
- London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online
- Thinkuknow provides support for parents and carers to keep their children safe online • Parentzone provides help for parents and carers on how to keep their children safe online
- UK Safer Internet Centre provide tips, advice, guides and other resources to help keep children safe online

---

Approved: December 2025 **Next review**: November 2026