Online Safety Policy

Approved via Governorhub

Approved date	**2 December 2025**
Review date	**December 2026**

Online Safety Policy

Aim
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

Legislation and Guidance
This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and 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.

This policy complies with our funding agreement and articles of association.

Roles & Responsibilities
The Governing Body
The Trust board have delegated the responsibility and monitoring of online safety to each of its Local Governance Committees. The Local Governance Committee is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy annually and in response to any internet safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure Internet safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

- Appoint a link governor to have overall responsibility for the governance of Internet Safety at the school who will:
  - Keep up to date with emerging risks and threats through technology use.
  - Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.
  - Chair the internet safety Committee

Headteacher
Reporting to the Local Governance Committee, the Headteacher has overall responsibility for internet safety within our school. The day-to-day management of this will be delegated to a member of staff, the internet safety Officer (or more than one), as indicated below.

The Headteacher will ensure that:

- Internet Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. pupils, all staff, senior leadership team and governing body, parents.
- The designated internet safety officer(s) has had appropriate Continued Professional Development (CPD) in order to undertake the day to day duties.
- All internet safety incidents are dealt with promptly and appropriately.
- All incidents of sexting are dealt with through the Safeguarding and Child Protection policy and procedures.

Internet safety Officer

The day-to-day duty of internet safety officer is devolved to *Christopher Scales, (Headteacher/DSL) and Charlotte Brattan (Online Safety Lead/DDSL)*

- Keep up to date with the latest risks to children whilst using technology; familiarise himself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher, governing body on all internet safety matters.
- Engage with parents and the school community on internet safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Liaise with Child Protection Designated Personnel on incidents of internet safety issues
- Ensure any technical internet safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or computing Technical Support.
- Make herself aware of any reporting function with technical internet safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

Computing Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
    - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
    - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
    - Any internet safety technical solutions such as Internet filtering are operating correctly.
    - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the internet safety officer and Headteacher.
    - Passwords are applied correctly to all users regardless of age. Passwords for staff will be subject to change every 3 months.
    - Pupil passwords, as children only use the network under supervision do not need changing.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.

- Any internet safety incident is treated as a Child Protection matter and appropriate measures taken. If you are unsure the matter is to be raised with the internet safety Officer or the Headteacher to make a decision.

All Pupils
The boundaries of use of computing equipment and services in this school are given in the pupils Acceptable Use Policy; any deviation or misuse of computing equipment or services will be dealt with in accordance with the behaviour policy.

Internet safety is embedded into our curriculum; pupils will be given the appropriate advice and guidance by staff. Similarly all pupils will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers
Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents' evenings, school newsletters, information on the school website and an annual parent's internet safety event, the school will keep parents up to date with new and emerging internet safety risks, and will involve parents in strategies to ensure that pupils are empowered.

Parents must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student Acceptable Use Policy before any access can be granted to school computing equipment or services.

Definitions
Users - refers to staff, governing body, school volunteers, pupils and any other person working in or on behalf of the school, including contractors.
Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.
School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.
Wider school community – pupils, all staff, governing body, parents and other relatives.
Safeguarding is a serious matter; at our school, we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as internet safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an internet safety incident, whichever is sooner.
The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

Technology
A range of devices maybe used in school including Chromebooks, PC's, laptops, iPads, Kindle Fire. In order to safeguard pupils and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering

We use an Enhanced Web Filtering Service provided by our IT provider Prism, that prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The computing Coordinator and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering
We use Gmail for education that prevents any infected email to be sent from the school or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Encryption
All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of a device such as laptop or iPad) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the DPO to ascertain whether a report needs to be made to the Information Commissioner's Office.

Passwords – all staff and pupils will be unable to access any device on the network without a unique username and password which is the same as the username and password for their Google Account. Staff passwords will change on a 3 monthly basis or if there has been a compromise, whichever is sooner. Passwords have been set up to autochange. Pupil passwords will not be changed unless a security breach has been identified and reported to the computing leaders. Devices that are not password enabled such as an iPad should be cleared of all personal data and files after use. Staff must ensure that Find my Ipad is enabled if their device is not on the school mdm system and is disabled prior to returning the iPad to school, which will allow staff members to redeploy the device without requesting personal passwords.

Anti-Virus
All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns. All USB peripherals such as key drives are not to be used in school or for school related work.

Safe Use
Internet
Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this internet safety and the staff Acceptable Use Policy; pupils upon signing and returning their acceptance of the Acceptable Use Policy.

Google Suite for Education
Pupils are permitted to use Google Suite for Education and will be issued with their own school-based Google account. All school online activity should be done through this system and monitored in the first place by the class teacher. Staff should be proactive in teaching the children to be responsible online citizens and encouraging positive online activity and reactive to deal appropriately with any misuse. Safeguarding & Child protection procedures should be followed where necessary.

Email

All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly, use of personal email addresses for work purposes is not permitted.
At present pupils do not have access to the email feature although this could be activated should it be required.

Photos and videos
Digital media such as photos and videos are covered in the schools' Mobile Phone and Camera Use Policy, and is re-iterated here for clarity. All parents have an option to refuse permission for their child to be photographed or videoed when they join the school and have the option to change their preferences at any time by informing the school in writing.

Social Networking
There are many social networking services available; our school is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within our school and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the Online Safety Officer who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- School website
- Facebook
- Class Dojo

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be "followed" or "friended" on these services and as such no two-way communication will take place.

In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of pupils using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be monitored by the class teacher or page host.
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Instant Chat and Message Apps

The minimum age to use these apps is 13 years old. If school becomes aware of use of these apps by pupils, who are under the minimum age, then the parents/carers will be contacted by the DSL/DDSL

Pupils, especially those in the older year groups choose to communicate with each other and with online 'friends' using instant messaging and chat apps like Instagram and WhatsApp? Although there are no plans to use these tools in school, teachers should be aware of their use and be prepared to

deal with any potential issues as they arise. Adults in school should not underestimate the power of these apps and the potential influence that they have on the lives of the young people in school. Open and frank discussions about online responsibility should take place throughout the school year not just in designated internet safety sessions.

Live Streaming

The increased popularity of 'Live Streaming' is an area that all staff should be mindful of, due to the potential of abuse. Although this activity should not be taking place in school it is still an area where staff will need to be vigilant. All staff should be prepared to discuss this in a neutral way through internet safety sessions.

Notice and take down policy
Should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents
Any Online Safety related incident are to be brought to the immediate attention of a Designated Safeguarding Officer, or their Deputy. The incident should be dealt with in the same way as any other Safeguarding & Child Protection concern and the relevant form completed and filed.

Any issues concerning the production and distribution of sexting images involving anyone under the age of 18 is illegal and needs careful management for all those involved. If a device is involved it will be confiscated and set to flight mode, where possible, or switched off while investigations are carried out.

Radicalisation and Extremism
All staff are aware through the annual staff PREVENT training of their roles and responsibilities in reducing the potential for groups or individuals of becoming involved in potentially extreme groups. Any suspicions must be dealt with immediately using the school child protection policy and referred to the police as appropriate.

Cyber-bullying
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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

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. Class teachers will discuss cyber-bullying with their tutor groups.

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, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school will also provide relevant 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from an appropriate member of staff (for example DSL/headteacher)
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to a member of the senior leadership team/DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably

practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Schools behaviour policy.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Links to other policies

Acceptable Use Code of Conduct

Camera & Mobile Devices

Safeguarding & Child Protection