The Oak Partnership

Online Safety Policy

We are committed to safeguarding and ensuring the health, safety and well-being of all pupils in accordance with safeguarding procedures and guidance for staff outlined in the schools' Health and Safety, Child Protection, Security and Safeguarding policies.

Document Information

	Information
Document author:	COO
Review by:	Board of Directors
Approved by:	Chair of Board of Directors
Adopted date:	17 December 2025
Publication date:	2023
Review schedule:	Annual
Distribution:	Trust website (linked on school websites)
Document status:	Version 3.0

Version Control

Version	Issue Date	Amended by	Comments
1.0	September 2021	TEBM	N/A
2.0	December 2024	COO	Policy re-written in entirety using The Key and SWGfl templates to inform/
3.0	December 2025	COO	Added that pupils are not permitted to use their own devices on school site. AI section 8 new.

1. Aims and Scope

Our schools aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, local school committee members and directors.
- Identify and support groups of pupils that are potentially at greater risk of harm online than others.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

This Online Safety Policy applies to all members of a school community (including staff, learners, local school committee members, directors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as 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, such as 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

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) 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
- Searching, screening and confiscation

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.

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

3. Roles and responsibilities

3.1 The Board of Directors

The Board of Directors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

3.2 Local School Committees

The Local School Committee must ensure:

- Schools have a system to ensure their school staff are receiving (at least) basic cyber-security training annually to ensure the school meets the DfE Cyber-Security Standards

- Schools review the DfE filtering and monitoring standards, and discuss with IT staff and service providers for their school what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies been put in place that meet their safeguarding needs.

The member of the Local School Committee who will take on the following responsibilities is the Nominated Safeguarding Governor. Most of these requirements will be fulfilled through safeguarding workstreams in Learning Review Weeks.

3.3 The headteacher

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

3.4 The designated safeguarding lead (DSL)

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher to review implementation of this policy annually
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the IT service provider for their school to make sure the appropriate systems and processes are in place
- Working with the headteacher, IT service provider and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged on CPOMs and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged on CPOMs and dealt with appropriately in line with the school behaviour policy
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher through safeguarding updates

- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.5 The IT Service Provider

The DfE Filtering and Monitoring Standards says:

> *"Senior leaders should work closely with local school committee members and directors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider."*
>
> *"Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support."*
>
> *"The IT service provider should have technical responsibility for:*
>
> - *maintaining filtering and monitoring systems*
> - *providing filtering and monitoring reports*
> - *completing actions following concerns or checks to systems"*
>
> *"The IT service provider should work with the senior leadership team and DSL to:*
>
> - *procure systems*
> - *identify risk*
> - *carry out reviews*
> - *carry out checks"*

If the school has a technology service provided by an outside contractor, it is the responsibility of the school to ensure that the provider carries out all the online safety measures that the school's obligations and responsibilities require. It is also important that the provider follows and implements school Online Safety Policy and procedures.

The IT Provider is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority / MAT or other relevant body
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the school's Head Teacher for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person (see appendix 'Technical Security Policy template' for good practice).
- monitoring systems are implemented and regularly updated as agreed in school policies

3.6 All staff and volunteers

All staff are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing
- Following the correct procedures by alerting a senior manager if they need to bypass the filtering and monitoring systems for educational purposes
- 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
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.7 Parents/carers

- Notify a member of staff if they have any concerns about online safety with their child or other children within the school.

Parents and carers are encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school.
- the safe and responsible use of their children's personal devices in the school (where this is allowed)

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum as set out in the appropriate Trust curriculum document.

Curriculum Leads will develop a planned and coordinated online safety education programme.

This will be provided through:

- a discrete programme
- PHSE and SRE programmes
- A mapped programme

- assemblies and pastoral programmes as required
- through relevant national initiatives and opportunities e.g. Safer Internet Day

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and/or in information via their website or virtual learning environment (VLE). This policy will also be shared with parents/carers via a link on each school's website.

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

-What are the issues? – UK Safer Internet Centre

-Hot topics – Childnet

-Parent resource sheet – Childnet

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 1 person or group by another person or group, where the relationship involves an imbalance of power.

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 (PSHE) education, and other subjects where appropriate.

All staff, local school committee members, directors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

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.

7.0 Pupil electronic devices

Pupils are required to hand in personal devices on arrival for school unless they need it for medical reasons.

The headteacher, and any member of staff authorised to do so, 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 the headteacher.
- Seek the pupil's co-operation and explain why the device is being searched.

Authorised staff members may examine, or delete, 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, or delete, 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 the staff member in conjunction with the DSL / headteacher / other member of the senior leadership team 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.

Staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, the device will be handed to the police as soon as reasonably practicable.

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

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

8.0 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access.

The Oak Partnership Trust recognises that AI has many uses to help pupils learn but may also risks that need mitigating.

The Trust will support the education of staff and pupils around the use of AI to promote:

8.1 Ethical and Responsible Use of AI

- Pupils and staff must be taught to use AI tools (e.g. Chat GPT, Google Bard) responsibly.
- AI must not be used to create or share harmful, misleading, or inappropriate content.

8.2 Data Privacy and Security

- Personal, sensitive, or identifiable information about pupils, staff, or parents must **never** be entered into AI tools.
- AI systems used by the school must comply with GDPR and Trust data protection policies.

8.3 Academic Integrity

- AI-generated content must not be submitted as original work.
- Pupils should be taught how to use AI for learning support (e.g., idea generation) without breaching academic honesty.

8.4 Misinformation and Bias

- AI outputs may contain inaccuracies or bias. Pupils and staff should critically evaluate AI-generated information.
- Schools will provide guidance on fact-checking and recognising bias in AI responses.

8.5. AI-Related Safeguarding Risks

- AI can be misused for bullying, harassment, or creating deep fakes (including explicit content). Such actions will be treated as serious breaches under the behaviour policy.
- AI-assisted grooming, voice cloning, and fraud attempts must be reported immediately to the DSL.

8.6. AI in Monitoring and Filtering

- Any AI-based monitoring tools must be reviewed regularly by DSL and IT staff to ensure accuracy and fairness.
- Human oversight is required for all safeguarding decisions involving AI.

9. Acceptable use of the internet in school

All staff, volunteers and local school committee members and directors are expected to abide by our Trust Acceptable Policy

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, staff, volunteers, local school committee members, directors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the Trust Acceptable Use Policy.

10. Pupils acceptable use

Each school within the Trust will support their pupils to understand what acceptable use of the internet looks like in school or personal devices used on their school site. The approach taken will vary in each school depending on the age and needs of the learners. Learners will also be supported to understand the consequences of breaching these rules.

11. How the Trust will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, schools will follow the procedures set out in their behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the disciplinary policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training

All new staff members will receive training, as part of their safeguarding induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

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).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, threatening, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse

- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies 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.

Local school committee members and directors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- A school's Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- IT acceptable use policy