OPEN BOX
Education Centre
St. John's Road, Epping, Essex, CM16 5DN
01992 577 300 info@openboxeducation.org.uk

Online Safety Policy

1. Purpose

Our school aims to:

- Have robust processes in place to ensure the online safety of students, 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, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

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 Principals 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 students' electronic devices where they believe there is a 'good reason' to do so.

3. Roles and Responsibilities

3.1 The Governors

The Governors have overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

The governors will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governors will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard students.

The Governors will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL). See Appendix 2.

The governors should ensure students are taught how to keep themselves and others safe, including keeping safe online.
The governors must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those 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 in place that meet their safeguarding needs.

A member of the Governing Body has taken on the role of Online Safety Governor.

All governors 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

- Ensure that online safety is a running and interrelated theme while devising and implementing the whole school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Principal

The Principal 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 designated safeguarding lead (DSL) and deputy are set out in our child protection and safeguarding policy as well as 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 with the IT manager and other staff, as necessary, to address any online safety issues or incidents
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the IT manager to make sure the appropriate systems and processes are in place
- Managing all online safety issues and incidents in line with the school Child Protection Policy
- 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 Relationships and 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 Principal and/or Governors
- 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.

3.4 The IT Manager

The IT Manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure students are kept 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 half termly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- 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 dealt with appropriately in line with the school Relationships and Behaviour Policy

This list is not intended to be exhaustive.

3.5 All Staff and Volunteers

All staff, including contractors, 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 students 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 Relationships and 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.

3.6 Parents and Carers

Parents and carers are expected to:

- Notify the Principal 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 (appendix 1)

Parents and 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

3.7 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.

4. Educating Students about Online Safety

Students will be taught about online safety as part of the PSE Curriculum:

Students 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
- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)
- The similarities and differences between the online world and the physical world, including: the impact of unhealthy or obsessive comparison with others online (including

through setting unrealistic expectations for body image), how people may curate a specific image of their life online, over-reliance on online relationships including social media, the risks related to online gambling including the accumulation of debt, how advertising and information is targeted at them and how to be a discerning consumer of information online

- The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for the particular needs of specific students.

5. Educating Parents and Carers about Online Safety

The school will raise parents and carers' awareness of internet safety in letters or other communications home, and in information via the school's website. This policy will also be shared with parents and carers.

Online safety will also be covered with parents and carers during the referral process.

The school will let parents and carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents and carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal (DSL).

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 Relationships and Behaviour Policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students 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 students, 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 (PSE) education, and other subjects where appropriate.

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

The school also provides information on cyber-bullying to parents and carers 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 Relationships and Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among students, 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.

6.3 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Open Box Education Centre recognises that AI has many uses to help students learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Open Box Education Centre will treat any use of AI to bully students in line with our Anti-bullying Policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

Any use of artificial intelligence should be carried out in accordance with our Use of Artificial Intelligence Policy.

7. Examining Electronic Devices

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

- Poses a risk to staff or students, 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, the authorised staff member will:

- Make an assessment of how urgent the search is, and consider the risk to other students and staff

- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the student'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 the Principal 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 student 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 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 students 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 students' electronic devices will be dealt with through the school complaints procedure.

8. Acceptable Use of the Internet in School

All students, parents and carers, staff, volunteers and governors 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 students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

9. Students Using Mobile Devices in School

Students may bring mobile devices into school but are expected to hand these into the office during lesson time.

Any use of mobile devices in school by students must be in line with the acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school Relationships and Behaviour Policy, which may result in the confiscation of their device.

10. Staff Using Work Devices Outside School

All staff members are issued with a work laptop. The IT Manager is responsible for ensuring that all necessary security software is installed and working prior to the device being issued to the staff member. Staff are responsible for taking appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters.
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in the Staff Code of Conduct.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the IT Manager.

11. How the School Will Respond to Issues of Misuse

Where a student misuses the school's IT systems or internet, we will follow the procedures set out in Relationships and behaviour Policy and Child Protection 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 IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which 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 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, 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 students can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL, Deputy DSL, IT Manager and other relevant staff 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.

Governors 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 Policy.

13. Monitoring Arrangements

The IT Manager conducts weekly monitoring of website access and 'key word alerting', recording any findings on the Online Safety Incident Log (Appendix 2). Every half term, the IT Manager tests the filtering system is working on a staff laptop, student laptop, both on-site and off-site, recording findings on the Record of Filtering and Monitoring Checks document (Appendix 4).

The IT Manager alerts the DSL to any behaviour and safeguarding issues relating to Online Safety. The DSL logs any behaviour and safeguarding issues related to Online Safety and reports these termly to the HR and Safeguarding Committee.

This policy will be reviewed every year by the IT Manager. At every review, the policy will be shared with the Governors. The review will be supported by an annual risk assessment that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

14. Links with other policies

This Online Safety Policy is linked to our:

- Child Protection Policy
- Relationships and Behaviour Policy
- Staff Disciplinary Procedures
- Staff Code of Conduct
- Data Protection Policy and Privacy Notices
- Complaints Procedure
- Harmful Sexual Behaviour and Child-on-Child Abuse Policy
- Anti-Bullying Policy
- Use of Artificial Intelligence (AI) Policy

Member of Staff Responsible for Online Safety: Alison Dolan, DSL

Governor Responsible for Online Safety: Julie Lorkins, Safeguarding Governor

IT Support Manager: Tim Dolan

Approved by: ..... (Principal)..... (date)

Authorised by:..... (Chair of Governors) ..... (date)

To be reviewed every: 1 Year

Next review date: October 2026

Date of Review	Reviewed by	Ratified by Governors	Date of next review
Dec 2020 – version 1.0	Tim Dolan		November 2022
Sep 2022 – version 2.0	Tim Dolan	11-10-22	October 2024
Sep 2023 – version 2.1	Tim Dolan	21-11-23	October 2024
Oct 2024 – version 2.2	Tim Dolan	03-12-24	October 2025
Oct 2025 – version 2.3	Tim Dolan	18-11-25	October 2026

Appendix 1

IT Acceptable Use Agreement

Acceptable use of the school's IT facilities and internet: agreement for students and parents/carers	
Name of student:	

When using the school's IT facilities and accessing the internet in school, I WILL NOT:
• Use them for a non-educational purpose
• Use them without a teacher being present, or without a teacher's permission
• Use them to break school expectations
• Access any inappropriate websites
• Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
• Use chat rooms
• Open any attachments in emails, or follow any links in emails, without first checking with a teacher
• Use any inappropriate language when communicating online, including in emails
• Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo/video
• Share my password with others or log in to the school's network using someone else's details
• Bully other people, or use offensive, discriminatory or divisive language
• Use AI tools and generative chatbots (such as ChatGPT or Google Bard):
  ○ During assessments, including internal and external assessments, and coursework
  ○ To present AI-generated text or imagery as my own work
When using the school's IT facilities and accessing the internet in school, I WILL:
• understand that the school will monitor the websites I visit and my use of the school's IT facilities and systems.
• immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.
• always use the school's IT systems and internet responsibly.
• understand that the school will need to speak with my parents/carers if I do certain unacceptable things online, even if I'm not in school when I do them.	

Signed (student):	**Date:**
Parent/carer agreement: I agree that my child can use the school's IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's IT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2

ONLINE SAFETY INCIDENT LOG

Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident

Appendix 3

Open Box Education Centre – IT Filtering and Monitoring Summary

The school uses a range of software to ensure we meet our obligations to provide a safe and secure experience for our students and staff and to ensure that the school IT network is as secure as possible.

Microsoft 365 offers a secure environment for communication and document creation, storage, sharing and back up. All students, staff and governors have access to the Microsoft 365 environment. Training and guidance is provided for users.

The school uses the following range of security, filtering and monitoring software:

Internet Filtering

Cleanbrowsing offers internet filtering at the point of the router (DNS level filtering) so any device brought into the building (mobile / tablet etc) is protected if using the school's WiFi network. Different profiles are set for staff and each student has their own personalised profile. These are loaded locally on to each laptop and will provide the same level of filtering when laptops are taken off site and connected to a home network.

Real-Time Classroom Monitoring

NetSupport School offers flexible real-time monitoring and control of student PCs while they are on the school's premises using the school network. Specific websites can be approved or restricted for certain lessons. Other functions such as printing, audio, use of removable media can be restricted or allowed as appropriate.

E-Safety Filtering, Monitoring and Reporting

NetSupport DNA offers a comprehensive solution for managing IT assets both on and off site. It includes a very powerful e-safety mode which raises an alert when a keyword is typed or searched and can produce reports based on the category of concern or particular user. This ensures that the school can comply with the latest guidance and legal requirements on safeguarding. NetSupport DNA works on any network as it provides a secure link via an IP gateway on the school network. This means safeguarding alerts will continue to be raised during any remote learning scenario.

October 2024

Appendix 4

Record of Filtering and Monitoring Checks

Record of Filtering & Monitoring Checks

Internet Filtering Test (Half Termly)

Date	Device	Location	Cleanbrowsing	Testfiltering.com	Notes & Actions	Completed by

Usage and Keyword Monitoring (Weekly)

Date	Report	Actions	Completed by