



Online Safety Policy

Document Control

Confidentiality Notice

This document and the information contained therein is the property of Fable House. This document contains information that is privileged, confidential or otherwise protected from disclosure. It must not be used by, or its contents reproduced or otherwise copied or disclosed without the prior consent in writing from Fable House.

Document Details

Organisation:	Fable House
Current Version Number:	2
Current Document Approved By:	Sonia King and Jane Blackburn
Date Approved:	February 2026
Next Review Date:	February 2027

Document Revision and Approval History

Version	Date	Version Created By:	Version Approved By:	Comments
1.00	08/01/2025	Lizzy Latham	Sonia King and Jane Blackburn	
2.00	27/02/2025	Lizzy Latham	Sonia King and Jane Blackburn	Reviewed: no changes

Aims

Fable House aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers, visitors and members of the oversight board
- Identify and support groups of students 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

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](#).

3. Roles and responsibilities

3.1 The oversight board

The oversight board is responsible for ensuring this policy is being implemented consistently throughout the school and will undertake regular audits to ensure this is the case.

All oversight board members will:

- Ensure they have read and understand this policy
- Ensure that the implementation of this policy is differentiated and accessible to all students during their audits
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet set out in the ICT and Communications Policy

3.2 The CEO

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

The CEO 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 CEO will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The CEO should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The CEO 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 CEO will review the DfE filtering and monitoring standards, and discuss with the Designated Safeguarding Lead, IT staff and service providers 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 in place that meet their safeguarding needs.
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college 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

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) and deputy safeguarding lead are set out in our safeguarding policy, as well as relevant job descriptions.

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

- Supporting the CEO in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the CEO and oversight board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with ICT support to make sure the appropriate systems and processes are in place
- Working with the CEO, ICT support 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 safeguarding 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 and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary

- Providing regular reports on online safety in school to the CEO and/or oversight board
- Undertaking annual risk assessments that consider and reflect the risks children face
- 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 ICT Technician

The ICT Technician is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually 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 ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Consulting with the Designated Safeguarding Lead before allowing access to specific sites staff have requested for educational purposes

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems as outlined in our IT and Communications Policy
- 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 by emailing the DSL and Deputy DSL
- Working with the DSL to ensure 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 dealt with appropriately in line with the school behaviour policy and logged on CPOMS
- 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/carers

Parents/carers are expected to:

- Notify a member of staff or the CEO of any concerns or queries regarding this policy

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](#)

3.7 Visitors and members of the community

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

4. Educating students about online safety

Students will be taught about online safety as part of both our project based curriculum and discrete PSHE sessions.

Students on our **Maple Pathway** will be taught to:

Use the internet safely to access information

Recognise inappropriate content, contact and conduct, and know how to get help if feeling unsafe online

Recognise when images online (including on social media apps) may have been manipulated and how this can impact young people

Protect their personal information, privacy and online identity

When students move onto our **Beech Pathway** they will be taught to:

Understand the dangers of grooming, cat fishing and radicalisation through online interactions

Discriminate between fact and inaccurate/false information presented online and understand why individuals may present false information online

Understand the laws and implications of sharing inappropriate images online including through social media

Understand the danger of online scams and 'phishing'

Understand the potential implications of online gambling, including in app purchases

How to report a range of concerns

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

Teaching about safeguarding, including online safety, will be adapted for individual students taking into account their developmental level, SEND and any other relevant vulnerabilities including historical and ongoing safeguarding issues.

5. Sharing information with parents/carers about online safety

This policy will be shared with parents/carers via the Fable House website along with online safety support resources.

The DSL/Deputy DSL will liaise with parents should there be any concerns about an individual student's online safety.

If parents/carers have any queries or concerns in relation to online safety, these should be raised with the CEO and/or the DSL.

Concerns or queries about this policy can be raised with the CEO and/or the DSL.

6. Filtering and Monitoring arrangements

Fable House uses the Smoothwall filtering and monitoring system. All information searched for online through the Fable House internet connection passes through the Smoothwall filter to ensure any inappropriate content and websites are inaccessible to students, staff and anyone else using our internet connection.

All students and staff have personalised log in details for the Fable House internet. If any inappropriate content is searched for by a student or staff member, the DSL and deputy DSL receive an instant notification to enable investigation. All necessary incidents are recorded on CPOMS and followed up in line with safeguarding procedures.

The Smoothwall system automatically updates every 24 hours to respond to any changes to online risks.

Fable House's filtering and monitoring arrangements are designed to keep our students and staff safe without limiting access to necessary educational resources. We understand that use of the internet has the potential to be a useful learning tool. Should staff feel sites which are needed for learning are being blocked by the Smoothwall, they should get in touch with DSL who will decide if access should be granted.

7. How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour and safeguarding policies. 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 staff disciplinary procedures / staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident which may include reporting to the relevant external agency.

8. Policy Review

This policy will be reviewed annually by the DSL taking into consideration the annually updated Keeping Children Safe in Education guidance.

9. Links with other policies

This online safety policy is linked to our:

- Safeguarding policy
- IT and Communications Policy
- Behaviour policy
- Staff code of conduct

10. Relevant staff details

CEO: Sonia King

Designated Safeguarding Lead: Lizzy Latham

Acting ICT Technician: Craig Holdsworth