Online Safety Policy

Approved by:	SDT	**Date:**	September 2023
Signed by:		**Position:**	CEO
Last reviewed:	September 2023	**Next review due:**	September 2024

Monitoring arrangements

This policy will be reviewed annually, but may be reviewed earlier if deemed appropriate by the Chief Executive, Headteacher(s), Trustees or Governing Board(s).

Contents

1. Aims

Inclusion Education aims to:

- Have robust processes in place to ensure the online safety of learners, staff, volunteers and trustees
- Deliver an effective approach to online safety, which empowers us to protect and educate the organisational 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
- Have a safe and effective approach towards social media

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk, as identified in Keeping Children Safe in Education 2023:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, 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 scam

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education 2023 , Working together to Safeguard Childrenand its advice for schools and education settings on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyberbullying: 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 and Department for Education filtering and monitoring standards . Further information can also be found here UK Safer Internet Centre

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 cyberbullying 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.

3. Roles and responsibilities

3.1 The Trustees

The Trustee board has overall responsibility for monitoring this policy and holding the Chief Executive, Headteacher(s) and governing boards to account for its implementation.

The trustees will hold the Governing Board to account for ensuring that the Headteacher(s) implement it across the school/college.

All Trustees will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the organisation's ICT systems as outlined in this policy
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and learners with SEND 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
- Receive appropriate child protection safeguarding training at induction (including online) and this will be regularly updated thereafter. This training will equip them with the knowledge to provide strategic challenge to test and assure themselves that the safeguarding policies and procedures in place in the school(s)/college(s) are effective and support the delivery of a robust whole school approach to safeguarding

3.2 The Governing Board

The Governing Board will monitor this policy and hold the Headteacher(s) to account for its implementation.

The Governing Board will review online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL) and/or Headteacher.

All Governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the organisation's ICT systems as outlined in this policy
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and learners with SEND 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
- Receive appropriate child protection safeguarding training at induction (including online) and this will be regularly updated thereafter. This training will equip them with the knowledge to provide strategic challenge to test and assure themselves that the safeguarding policies and procedures in place in the school(s)/college(s) are effective and support the delivery of a robust whole school approach to safeguarding

3.3 Headteacher and SLT

Inclusion Education's Headteachers are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the organisation

The Headteachers have additional responsibilities related to the security protection and monitoring systems in place, namely:

- 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 pupils are kept safe from potentially harmful and inappropriate content and contact online while on Inclusion Education premises, including terrorist and extremist material
- Ensuring that the organisation''s ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Liaising and overseeing security checks and monitoring for the organisation's ICT systems with its network partners
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

The senior leadership team are responsible for:

- procuring filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of your provision
- overseeing reports

They are also responsible for making sure that all staff:

- understand their role
- are appropriately trained
- follow policies, processes and procedures
- act on reports and concerns

Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

This list is not intended to be exhaustive.

3.4 The designated safeguarding lead (DSL)

Details of each centre's designated safeguarding lead (Marie Greenhalgh and Matthew Atkinson) are set out in our child protection and safeguarding policies, as well as relevant job descriptions, and on Inclusion Education's website.

The DSL takes lead responsibility for online safety in their respective setting, in particular:

- Supporting the Chief Executive and Head(s) of Centre in ensuring that staff understand this policy and that it is being implemented consistently throughout the organisation
- Working with the Chief Executive, IT 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 organisation's child protection and safeguarding policies

- Ensuring that any online safety incidents are logged (see appendix 3) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the organisation's 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 to the Chief Executive, Head(s) of Centre and/or trustee board

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
- Adhering to the terms on acceptable use of the organisation's ICT systems and the internet (**3.5.1**), and ensuring that learners follow the organisation's terms on acceptable use (**3.7**)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 1) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are dealt with appropriately in line with the organisation's 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.

3.5.1 Acceptable use

The following is Inclusion Education's acceptable use for its trustees, staff, volunteers and other visitors ("Staff"). All those aforementioned should:

- Always use the Inclusion Education's ICT systems and internet responsibly, and ensure that learners in their care do so too and that they should not access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use the organisation's ICT systems and access the internet for educational purposes or for the purpose of fulfilling the duties of my role.
- Understand that the organisation will monitor the websites visited and usage of the organisation's ICT facilities and systems.
- Take all reasonable steps to ensure that work devices are secure and password-protected when using them outside Inclusion Education premises, and keep all data securely stored in accordance with this policy and the Inclusion Education's data protection policy.
- Should use an Inclusion Education device when accessing information related to the organisation's work at home

- Inform the designated safeguarding lead (DSL) and Headteacher know if a learner informs then they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material
- Not use Inclusion Education devices, network or other ICT systems in any way which could harm the organisation's reputation
- Minimise accessing social networking sites or chat rooms, and using mobile devices, as part of positive role modelling, unless required by their role
- Not use any improper language when communicating online, including in emails or other messaging services
- Not install any unauthorised software, or connect unauthorised hardware or devices to Inclusion Education's network
- Protect their password from others and not log in to the organisation''s network using someone else's details
- Not take photographs of learners without checking with the Headteacher first
- Not share confidential information about the Inclusion Education, its learners or staff, or other members of the community
- Not access, modify or share data I'm not authorised to access, modify or share
- Not promote private businesses, unless that business is directly related to Inclusion Education.

3.6 Learners

Learners attending Inclusion Education and using the organisation's ICT systems and internet network will be be responsible for using that they:

- Always use the organisation's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a member of staff immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

As part of Inclusion Education's promotion of positive behaviour, as detailed in its Behavior Policy and Behaviour Curriculum, and commitment to providing an inclusive, diverse and safe environment for its learners and staff members they should not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless a member of staff has expressly allowed this as part of a learning activity
- 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
- Log in to the school's network using someone else's details

- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If a learners bring a personal device with them into one of the organisation's centre's:

- Staff will encourage the positive management of the device in session rather than its confiscation to help support the learner as part of the progress or preparation for the workplaceI will not use it during sessions without a teacher/tutor's agreement
- However, staff may have to speak with parents/carers and form written agreements to support the positive management of a device, such as handing this to a member of staff at the start of the session to be returned before departure
- They will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

3.7 Parents/carers

Parents and carers are expected to:

- Notify a member of staff or the relevant Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and complies with all that set out in section 3.7

Parents 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 International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

3.8 Visitors and members of the community

Visitors and members of the community who use the organisation'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 (appendix 2).

4. Online communication and safer use of technology

4.1 Managing the Inclusion Education website

Inclusion Education will ensure:

- Information posted on our website is in line with that identified by the Department for Education (DfE) and the Charity Commission
- Our website complies with guidelines for publications including: accessibility, data protection, respect for intellectual property rights, privacy policies and copyright.
- Staff or learners' personal information will not be published on our website without explicit permission

- The website administrator account for the Inclusion Hampshire website will be secured with an appropriately strong password
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community

4.2 Publishing videos and images online

- Inclusion Education will obtain permission from parents/carers before images/videos of learners are electronically published.

4.3 Managing emails

- Learners may only use their Inclusion Education provided email accounts for educational purposes
- All staff are provided with an Inclusion Education email address to use for any official communication. The use of personal email addresses by staff for any official Inclusion Hampshire communication is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any member of the Inclusion Education community (staff or learner) should speak with the Chief Executive, Headteacher or DSL if they receive an offensive, discriminatory or prejudiced communication.
- Sensitive or personal information will only be shared via email in accordance with data protection legislation.
- Email sent to external organisations should be written carefully before sending with particular attention paid to the recipient address to avoid a data breach.
- Inclusion Education email addresses and other official contact details should not be used for setting up personal social media accounts or subscribing to services.

4.4 Safe use of the internet during sessions

- All staff are aware that they cannot rely on filtering alone to safeguard learners and supervision, classroom management and education about safe and responsible use is essential (see Section 6)
- Alongside network filtering and monitoring, Inclusion Education implements the “Ripple tool” extension from Ripple Suicide Prevention (https://www.ripplesuicideprevention.com/) to safeguard its learners and support their mental health and wellbeing. This tool is implemented automatically across all Inclusion Education Chromebook devices and initiated when a search term related to self-harm and suicide is used. When triggered, it will offer a message of hope, a breathing technique and signpost to further support.
- Learners will be appropriately supervised when using technology, according to their ability and understanding.
- Inclusion Education will use the internet to enable learners and staff to communicate and collaborate in a safe and secure environment.

- Internet use is a key feature of educational access and all learners will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded curriculum.
- Learners will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Learners will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

4.5 Management of platforms and systems

- The Senior Leadership Team and staff will regularly monitor the usage of its learning platforms and systems by learners and staff in all areas, in particular message and communication tools.
- The Trustees, Governing Body and Headteachers should ensure that the school and college has appropriate filters and monitoring systems in place and regularly review their effectiveness
- When staff and learners leave Inclusion Education their account or rights to specific Inclusion Education systems (such as Gmail and Google Workspace) will be disabled. Staff and learners will be informed in advance so they have time to retain resources but are strictly forbidden from retaining personal details or information that may have been available to them whilst at Inclusion Education
- Any concerns about content on Inclusion Education platforms and systems may be recorded and dealt with in the following ways:
    - The user will be asked to remove any material deemed to be inappropriate or offensive.
    - The material will be removed by the site administrator if the user does not comply, access to the platforms/systems for the user may be suspended.
    - The user will need to discuss the issues with the Headteacher before reinstatement. A student's parent/carer may be informed.

5. Social Media Policy

Expectations regarding safe and responsible use of social media will apply to all members of the Inclusion Education community and exist in order to safeguard both the organisation and the wider community, on and offline. Examples of social media may include websites such as Instagram, Snapchat, Facebook, TikTok, blogs, wikis, other social networking apps/websites, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.

All members of the Inclusion Education community:

- will be encouraged to engage with social media in a positive, safe and responsible manner at all times.
- will be provided with information about safe, appropriate and responsible use of social media. This will be communicated clearly and regularly to learners as part of the curriculum and to staff in training and other communications.
- are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others as part of Inclusion Hampshire's promotion of kindness, positive mental health and wellbeing.

- should report any concerns regarding the online conduct of any member of the Inclusion Education community on social media sites should be reported to the Headteacher/DSL and will be managed in accordance with existing policies such as anti-bullying, allegations against staff, behaviour, low-level concerns, safeguarding/child protection.

5.1 Staff personal accounts

Staff are entitled to have their own personal social media accounts(s), which , by definition, must remain personal. Personal social networking should be kept separate from any Inclusion Education related activities. In particular, personal account users must:

- Avoid making any negative references to Inclusion Education or anyone associated with the organisation
- Not make “friends”, “follow” or otherwise communicate through social media with learners or anyone who could be deemed a user of any of Inclusion Education’s services without explicit consent of the Chief Executive or Headteacher(s).

5.2 Inclusion Education accounts

Inclusion Education has an official presence on social media platforms. Any future presence on new or emerging platforms can only be set up with the written authority of the Chief Executive.

- All Inclusion Education social media accounts must have a specific purpose aimed at supporting one more of the following areas of Inclusion Hampshire’s work:
- Promoting Inclusion Education
- Promoting a particular service, project or event which Inclusion Education supports as part of its ongoing mission
- Fundraising for Inclusion Education

All official social media accounts must contain the name ‘Inclusion Education ’ or, where there are character limitations, or that name is unavailable an alternative will be agreed by the Chief Executive.

All official social media accounts will have a nominated authorised user. In most cases, this will be Inclusion Hampshire Education’s communications officer. The authorised user accepts the responsibility for representing Inclusion Education in a professional manner and is personally responsible for ensuring that:

- He/she/they understand and comply with the terms of service of the social media platform. He/she/they are responsible for signing or otherwise agreeing to abide by the terms of services.
- If possible, he/she/they attend appropriate training on the best use of social social to promote Inclusion Education
- All content on the site is appropriate, accurate and adding value
- All mistakes and or inaccuracies, should they be identified, should be reported to the communications officer for immediate correction.
- All external posts that are considered offensive and/or negative must be brought to the attention of the Chief Executive and should not receive a response
- All information posted should comply with Inclusion Education ’s policies, particularly those governing confidentiality and data protection

- Individuals, no matter their status or relationship to Inclusion Education , must not be referenced without their written consent. This includes all photos, videos and other media.
- Copyright laws and intellectual property rights must be respected by the authorised user.
- Any posts expressing a personal view including appropriate caveats, e.g. these views are personal and do not do not necessarily represent the views of Inclusion Education ”
- Content should be monitored across all platforms weekly
- Social media is not used for the conduct of Inclusion Education business and should be contacted through appropriate channels (e.g. letter or email)
- Inclusion Education will retain copies of all login details and passwords used to access its social media accounts
- The maintenance of social media accounts cannot be delegated by the authorised user without strict supervision and the authorised user will remain responsible and accountable for any content posted

6. Educating learners about online safety

Inclusion Education ’s learners will be taught about online safety as part of its curriculum:

In **Key Stage 3**, learners will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Learners in **Key Stage 4** 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

By the **end of secondary school, or KS5,** learners will know:

- 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 safe use of social media and the internet will also be covered in other subjects, where relevant, as part of the organisation's commitment to the Spiritual, Moral, Social and Cultural (SMSC) development of its learners.

Teaching about safeguarding, including online safety, will be designed with the needs of those who are most vulnerable, victims of abuse and learners with SEND whilst remaining applicable to all. If necessary, this will be adapted by members of staff.

6. Educating parents and carers about online safety

Inclusion Education will raise parents/carers' awareness of internet safety in letters, emails, or other communications home, via our website, social media or virtual learning environment (VLE) and as part of its pastoral care. This policy will also be shared with parents/carers.

Inclusion Education will let parents/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/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the relevant Headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

7. Cyberbullying

7.1 Definition

Cyberbullying 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. Please see Inclusion Education s Anti-Bullying and Behaviour Policies for further information on how the organisation prevents and addresses bullying, including cyberbullying, in all its forms.

7.2 Examining electronic devices

Inclusion Education staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on learners'' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or

- Disrupt teaching, and/or
- Break any of the organisation's rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a learner discloses that they are being abused and that this abuse includes an online element.

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

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The organisation's COVID-19 risk assessment

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

8. Learners using mobile devices

Learners may bring mobile devices into Inclusion Education 's sites, but should not use them during sessions unless specifically allowed as part of teaching and learning, therapeutic activity or for reasons of safety.

Any use of mobile devices on the organisation's premises by learners must be in line with section 3.7 of this policy. Any breach of the acceptable use agreement by a learner may trigger action in line with the organisation's behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices inside and outside of the organisation's premises

All staff members will take 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 (e.g. asterisk or currency symbol) or are long passphrases (e.g. Bats-Jellied8-Overfull-Economist)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device is proactively locked by the member of staff using the device, or that it locks left inactive or unattended for a short period of time
- Not sharing the device among family or friends
- Ensuring a firewall system is in place (such as Windows Defender), an anti-virus system is installed (such as Malware Bytes) and that no suspicious and phishing websites are visited
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the organisation's terms of acceptable use, as set out in appendix 1 and 2.

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 their line manager.

10. How the organisation will respond to issues of misuse

Where a learner misuses the organisation's ICT systems or internet, it will follow the procedures set out in the organisation's behaviour policy and its and the ICT and internet acceptable use. 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 organisation'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 and staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyberbullying 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, bulletins/newsletters 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 pupils can recognise dangers and risks in online activity and can weigh the risks up
- 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, and at least annually.

Trustees 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 policies.

12. Monitoring arrangements

All staff log behaviour and safeguarding issues related to online safety which is monitored and reviewed daily by the safeguarding team. An example concern log can be found in appendix 1.

This policy will be reviewed every year by the Chief Executive. At every review, the policy will be shared with the trustee board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection policy
- Safeguarding policy
- Behaviour policy
- Anti-bullying policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1: online safety concern log

Concern type All

Date	Concern	Concern type	Member of staff reporting	Actions and notes
		Social media/internet safety		