Online Safety Policy

Approved by:	Trustee Board	**Date:**	August 2025
Signed by:	AS Minshull - Beech	**Position:**	Chair
Last reviewed:	August 2025	**Next review due:**	September 2026

Monitoring arrangements

This policy will be reviewed **annually** by the designated Head and DSL. At every review, it will be approved by the Inclusion Education's Trustee board.

Author: Matthew Atkinson	Title: Online Safety policy	Ref: IE-H&S03	Date: September 2025
Inclusion Education is the working name of Inclusion Hampshire CIO registered number 1162711			

Contents

The Inclusion Way’TM : A Shared Foundation

‘The Inclusion Way’ has been developed by Inclusion Education and is based on over ten years’ experience. ‘The Inclusion Way’ captures our ethos to wellbeing and mental health, our pedagogical approach and all aspects that affect a learner’s educational experience.

This introduction outlines how the ‘Inclusion Way’ is used and embedded as a shared vision and foundation across all our policies and practices at Inclusion Education. This introduction defines who our learners are, why they are here, and how our inclusive pedagogical approach ensures our they are supported, valued and empowered.

It is important to understand the journey our typical learner has been on before they arrive at Inclusion Education.

For example, our learners will:

- typically have a severe and chronic diagnosed mental health need. They are likely experiencing, or have experienced, self-harm, suicide ideation, depression, and high anxiety.
- have diagnosed and/or undiagnosed SEND needs related to speech, language and communication (SLCN), communication and interaction (C&I), or specific learning differences (SpLD).
- often experience significant gaps in education at primary and/or secondary level.
- have a history of non-attendance due to high anxiety and mental health needs and have been identified as emotionally based school avoiders (EBSA).
- are often working below age-related expectations in Maths, English, and Science due to disrupted education and unmet needs.
- may have experienced trauma, whether through Adverse Childhood Experiences (ACEs) or bullying in previous educational settings.
- are young people exploring their identity and discovering who they are and who they want to be. While they may struggle with emotional regulation or academic attainment, they are not of primary-age cognitive ability, they are young adults and want to be treated as such.

‘The Inclusion Way’ is more than a framework: it is the heart of our mission. By addressing mental health, SEND, and academic development as equally essential, we equip young people not only to succeed in education but to thrive in life. Our learners tell us this works. Their progress shows us it works.

* Learners is used throughout this document and refers to learners, students and young people attending settings and using services

2. Aims

Inclusion Education aims to:

- Have robust processes in place to ensure the online safety of learners, staff, volunteers and trustees/governors
- Identify and support groups of learners 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 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 2025:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, 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 scam.

3. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education 2024, and 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.

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

4. Roles and responsibilities

4.1 The Trustees

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

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

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 schools/college are effective and support the delivery of a robust whole schools/college approach to safeguarding

4.2 The Governing Board(s)

The governing board(s) 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 governing board(s) 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 children.

The governing board(s) 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 governing board(s) should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board(s) must ensure the schools/college has appropriate filtering and monitoring systems in place on schools/college devices and schools/college 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 schools/college 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.

The named trustee for online safety and safeguarding is Jane Pratt

4.3 Head of Setting

Heads are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the organisation

The Head has 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 learners 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

This list is not intended to be exhaustive.

4.4 The designated safeguarding lead(s) (DSL)

Details of the designated safeguarding lead are set out in the child protection and safeguarding policy, 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 Head in ensuring that staff understand this policy and that it is being implemented consistently throughout the schools/college
- Working with the head and governing 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 schools/college devices and schools/college networks
- Providing governors with assurances that filtering and monitoring systems are working effectively and reviewed regularly
- Working with Inclusion Education's IT provider to make sure the appropriate systems and processes are in place
- Working with the headteacher, 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
- Responding to safeguarding concerns identified by filtering and monitoring
- Ensuring that any online safety incidents are logged 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
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Providing regular reports on online safety to the Headteacher and Local Governing 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.

4.5 Inclusion Education’s IT provider

Inclusion Education’s COO, working with the organisation’s IT provider, GreenPoint, is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on schools/college devices and schools/college networks, which are reviewed and updated at least annually to assess effectiveness and ensure learners are kept safe from potentially harmful and inappropriate content and contact online while at schools/college, including terrorist and extremist material
- Ensuring that the schools/college’s ICT 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 schools/college’s IT systems on a half-termly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

This list is not intended to be exhaustive.

4.6 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 to acceptable use of the organisation’s ICT systems and the internet, and ensuring that learners follow the organisation’s terms on acceptable use
- 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 contacting the Headteacher and raising a ticket with the GreenPoint service desk.
- Following the correct procedures by raising a ticket 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 (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.

4.7 Learners

Learners attending Inclusion Education and using the organisation’s ICT systems and internet network will be responsible for abiding by the acceptable use of the internet agreement outlined here:

- 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 their username and passwords safe and not share these with others
- Keep 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 Behaviour Policy, 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 schools/college'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 computer (excluding mobile phone) with them into one of the organisation's centres:

- Staff will encourage the positive management of the device in session rather than its confiscation to help support the learner/student as part of the progress or preparation for the workplace 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.

4.8 Parents/carers

Parents and carers are expected to:

- Notify a member of staff or the relevant Head of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the schools/college's ICT systems and interne
- 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

4.9 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 and expected to read and follow it. If appropriate, they will be expected to agree to the terms set out on signing in (via the Sign In App).

5. 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/student 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 unless explicitly authorised to do so by the Headteacher, COO or CEO using authorised Inclusion devices
- 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.

5.1 Safe use of the internet during learning

- 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)
- 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.

5.2 Management of platforms and systems

- The Senior Leadership Team(s) 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(s) and Head(s) should ensure that the schools/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 Microsoft 365) 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 Head before reinstatement. A learners parent/carer may be informed.

5.3 Filtering and monitoring arrangements

Inclusion Education, in partnership with GreenPoint, the organisation's IT provider, has robust filtering and monitoring arrangements in place to safeguard its learners.

- **Filtering**

  The schools use Smoothwall filtering to log and block, as appropriate, all traffic for all devices accessing Inclusion Schools' WiFi. This applies to staff, learners and visitors and all devices – mobile devices, laptops and computers.

  There are two configurations for staff and learners in which staff have access to more content that is otherwise blocked for learners. For example, learners cannot access YouTube but staff can in order to access educational content.

  Our IT provider provides weekly summary reports to the DSL.

  If a website needs to be blocked, this can only be authorised by the Headteacher or DSL.

- **Monitoring**

  The schools use Smoothwall's Monitor programme which is deployed to all devices (excluding mobile policies).

  If anyone was to type something using an Inclusion Education device this may be logged and sent to a member of the safeguarding team (if it is of a serious enough nature, Level 3+). However, even Level 1 or 2 concerns are logged and reviewed by the safeguarding team.

  It should be noted that this applies to all staff and learners.

6. Educating learners about online safety

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

All schools have to teach:

- Relationships and sex education and health education in secondary schools

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 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, 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.

7. Educating parents and carers about online safety

Inclusion Education will raise parents/carers' awareness of internet safety in letters, newsletters, emails, or other communications home, via our website, social media 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 schools/college 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 schools/college (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.

8. Cyberbullying

8.1 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.

8.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that learners understand what it is and what to do if they become aware of it happening to them or others. We will ensure that learners know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The schools/college will actively discuss cyber-bullying with learners, explaining the reasons why it occurs, the forms it may take and what the consequences can be. This happens in timetabled lessons, in tutor time and in 1:1 with a member of the wellbeing team or a member of SLT.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support learners, as part of safeguarding training (see section 11 for more detail).

The schools/college also sends information/leaflets on cyber-bullying to parents/carers so 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 schools/college will follow the processes set out in the schools/college behaviour policy. Where illegal, inappropriate or harmful material has been spread among learners, the schools/college 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.

8.3 Examining electronic devices

The Headteacher(s) and any member of staff authorised to do so by the Headteacher(s), can carry out a search and confiscate any electronic device they have reasonable grounds of suspecting:

- Poses a risk to staff or learners, and/or
- Is identified in the schools/college 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 learners and staff. If the search is not urgent, they will seek advice from the headteacher or a member of the safeguarding team
- Explain to the learner/student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the learner/student's co-operation.

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 schools/college 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 Headteacher, DSL or other member of the senior leadership team to decide 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 learner/student and/or the parent/carer refuses to delete the material themselves.

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

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

Any searching of learners 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
- Our behaviour policy.

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

8.4 Artificial Intelligence (AI)

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

Inclusion Education recognises that AI has many uses to help pupils 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.

Inclusion Education will treat any use of AI to bully learners in line with our anti-bullying and behaviour 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 Inclusion Education.

9. Learners using mobile devices

Please refer to each setting's mobile device policy for information on devices.

Any use of mobile devices on the organisation's premises by learners must be in line with section 4 of this policy. Any breach of the acceptable use agreement by a learner/student may trigger action in line with the organisation's behaviour policy, which may result in the confiscation of their device.

10. 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 12 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol) or are long passphrases made of 3 or 4 random words (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.

Work devices must be used solely for work activities and are overseen by Inclusion Education’s IT partner, GreenPoint, in order to protect the security, privacy and integrity of the organisation’s devices.

If staff have any concerns over the security of their device, they must raise a ticket with the IT provider and inform the Headteacher.

11. How the organisation will respond to issues of misuse

Where a learner/student 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.

12. 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 learners can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence learners 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.

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 and safeguarding policies.

13. Monitoring arrangements

All staff log behaviour and safeguarding issues related to online safety on CPOMS which is monitored and reviewed daily by the safeguarding team.

This policy will be reviewed every year. 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 learners 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:

- Safeguarding & Child Protection policy
- Behaviour policy
- Anti-bullying policy
- Mobile Devices policy
- Data protection policy and privacy notices
- Complaints procedure
- Staff Code of Conduct
- Allegations against staff and low-level concerns