Surrey Teaching Centre

Kristin Hoogland

Date: October 2026

Review Date: October 2028

Online Safety Policy- Surrey Teaching Centre

Implications of an acquired brain injury

"Another common outcome from a frontal lobe injury is lack of awareness. This can make it difficult to analyse one's own behaviour or to assess other people's reactions. This complicates the issue of impulsivity, as the person may refuse to acknowledge that they have inappropriate behaviour. They may be unable to understand their own limitations, or the consequences of their actions. A person lacking in insight is also often unable to understand other people's behaviour or motives, and unable to empathise or imagine how someone else is feeling."(synapse 2014, The Brian Injury Association of Queensland)

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and management committee members
- 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

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, 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

Legislation and guidance

This policy is based on the Department for Education's (DfE) 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

It also refers to the DfE's guidance on:

- protecting children from radicalisation.
- RSE and health education

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.

Roles and responsibilities

The Management Committee

The management committee has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The management committee member who oversees safeguarding is Catherine Johnson.

All management committee members will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children and some pupils 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

The headteacher

- The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- The headteacher is also responsible for ensuring that:
  - the school has appropriate policies in place that make it clear that sexual harassment, online sexual abuse and sexual violence (including sexualised language) is unacceptable, with appropriate sanctions and support in place.
  - the school's staff have appropriate knowledge of part 5 the government's 'Keeping children safe in education' guidance.
  - children are provided with opportunities throughout the curriculum to learn about safeguarding, including keeping themselves safe online

The Headteacher is also responsible for ensuring that the ICT systems:

- Have an appropriate level of security protection, 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 at school, including terrorist and extremist material

- Are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Block access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

The designated safeguarding lead

The DSL is responsible for:

- Holding the lead responsibility for safeguarding and child protection in the school, this responsibility is not able to be delegated
- Understand the risks associated with online activity and be confident that they have the up to date knowledge and capability to keep children safe whilst they are online at school; in particular understand the additional risks that children with SEND face online and the associated and appropriate support they require
- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on CPOMs and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged on CPOMs and dealt with appropriately in line with the school behaviour policy
- 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 headteacher and/or management committee
- This list is not intended to be exhaustive.

All staff

All staff are responsible for:

- Knowing that sexual violence and sexual harassment exist on a continuum and may overlap; they can occur online and offline (both physically and verbally) and are never acceptable. It is important that all victims are taken seriously and offered appropriate support.

Responding to reports of sexual violence and sexual harassment

- Children making any report of sexual violence or sexual harassment including “up skirting” (The Voyeurism Offences Act 2019) will be taken seriously, kept safe and be well supported. If the report includes an online element staff will be mindful of the Searching, Screening and Confiscation: advice for schools 2018 guidance
- 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 and the internet and ensuring that pupils 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 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'

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Adhere to STC's Acceptable use of ICT agreement

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
- Keeping children safe online - Keeping Children Safe Online | NSPCC

Screen time and Screen use

Screen time refers to the amount of time a child spends looking at a screen. Screen use refers to how, why and in what context screens are used. It takes into account the quality and pace of content, purpose and level of engagement.

Screen use at STC is limited, carefully planned and clearly linked to intended learning aims. Screen-based assistive technology can be an important tool to help STC's learners communicate, take part in everyday activities, and create an inclusive learning environment.

Educating pupils about online safety

At Surrey Teaching Centre, all pupils have a special educational need. Therefore, teaching about safeguarding, including online safety, has been adapted to meet the needs of our learners and this is approached on an individual basis for each learner. For those students in early recovery it may not be appropriate or possible to cover any content of this nature. These students follow a sensory curriculum offer, where staff will model and support students to interact with technology safely and appropriately.

STC teaches children about our technologically diverse world by talking to them in an age-appropriate way about different types of technology and how to use them safely.

Pupils will be taught about online safety as part of the curriculum:

In the **Early Years**, pupils may be taught to (if appropriate and accessible):

- Develop an age-appropriate understanding of how to use digital technology safely, including recognising when something feels unsafe or uncomfortable and knowing to seek help from a trusted adult.

In **Key Stage 1**, pupils may be taught to (if appropriate and accessible):

- Use technology safely and respectfully, including understanding the importance of keeping personal information private.
- Recognise when something they see, hear or experience online may be concerning and know who to go to for help and support.

In **Key Stage 2**, pupils may be taught to (if appropriate and accessible):

- Use technology safely, respectfully and responsibly.
- Recognise appropriate and inappropriate online behaviour.
- Know how and where to seek help and report concerns about online content or contact.

In **Key Stage 3**, pupils may be taught to (if appropriate and accessible):

- Use technology safely, respectfully, responsibly and securely, including understanding how to protect their privacy and personal information.
- Recognise inappropriate content, contact and conduct, and know how to seek help and report concerns.

In **Key Stage 4/5**, pupils may be taught to (if appropriate and accessible):

- Understand how changes in technology can create new opportunities and risks, including the importance of protecting online privacy and personal information.
- Know how to seek help and report a range of online safety concerns.

Artificial Intelligence (AI) and Assistive Technology

STC recognises that artificial intelligence (AI) and assistive technologies can support teaching, learning, communication, accessibility and personalised provision for pupils with acquired brain injuries. Staff are encouraged to develop an appropriate understanding of these technologies and to consider how they can be used safely, ethically and effectively to support individual learners.

When using AI tools or assistive technology as part of their work, staff should consider the accuracy, appropriateness and accessibility of the information or resources produced, and retain professional oversight and judgement. Staff must not enter confidential, personally identifiable or sensitive information about pupils, families or colleagues into AI tools unless the use of that specific tool has been appropriately authorised. AI-generated content should be checked before being used with pupils, particularly where it may influence teaching, assessment, communication or decision-making.

Assistive technologies, including speech-to-text, text-to-speech, captioning, communication tools and other accessibility software, should be used in accordance with individual pupil needs and relevant school guidance. Staff should ensure that technology enhances rather than replaces professional interaction and should remain alert to issues relating to privacy, consent, digital security, bias and reliability.

Where appropriate, pupils should also be supported to develop an age- and ability-appropriate understanding of AI and digital technologies, including their benefits, limitations and the importance of using them safely and responsibly.

Educating parents about online safety

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

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

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

Cyber-bullying

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.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so.

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.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Staff using work devices outside school

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)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

Staff members must not use the device in any way which would violate the school's terms of acceptable use or 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 school's business manager.

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 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

And to learn that:

- Some adults and other children use these technologies to harm children. The harm might range from sending hurtful or abusive texts or emails, to grooming and enticing children to engage in extremist or sexual behaviour involving webcam photography or face-to-face meetings.
- Children may also be distressed or harmed by accessing inappropriate material such as pornographic websites or those which promote extremist behaviour, criminal activity, suicide or eating disorder
- Children with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime. If there are concerns about a child in this area, the DSL (or a deputy), will consider a referral into the Cyber Choices programme.
- This programme aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.
- Child sexual exploitation does not always involve physical contact; it can also occur through the use of technology. All staff are aware of the link between online safety and vulnerability to CSE.

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.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every 2 years by the Headteacher. At every review, the policy will be shared with the management committee. The review 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.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT 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 pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviours for effective learning policy
- Staff disciplinary procedures
- GDPR policy
- Complaints procedure
- Anti-bullying
- Curriculum Policy
- Personal Pathways Policy
- Recruitment and Selection
- Relationships, Sex and Health Education