Creating Excellence Together,
through a culture of care

BRIGANTIA LEARNING TRUST ONLINE SAFETY POLICY

BRIGANTIA
LEARNING TRUST
Creating Excellence Together,
through a culture of care

Document Control

Title:	Online Safety Policy
Policy Lead:	Director of Education
Category:	Safeguarding
Date Approved:	4th December 2025
Approved by:	Trust Board
Review Date:	December 2026
Review Period:	Annual
Status:	Statutory/~~Non-Statutory~~
Website:	Yes
Annual Agreement:	Yes

Review

Date:	Version:	Author:	Revisions:
Nov 2024	2	RB	5.2 - Added Commerce 7 - Added detail on the use of AI 8 – Added detail on the systems used
Nov 2025	3	DoE	Updated to incorporate key changes in line with updated exemplar polices from the Key for Leaders 1. Introduction – Categories of risk 2. Aims – Updated Roles And Responsibilities 4.2 Trust Executive 4.4 DSL 4.6 Staff and Volunteers 4.7 Parents and carers 5.1 Updated - Educating pupils about online safety 5.3 Updated - Educating parents about online safety

Contents

1. Introduction

Brigantia Learning Trust recognises the benefits and opportunities which new technologies offer to teaching and learning. The use of technology is encouraged to enhance skills and promote achievement. However, the accessible and global nature of the internet and variety of technologies available mean that the Trust is also aware of potential risks and challenges associated with such use. The Trust approach is to implement safeguards across the Trust and to support staff, children and young people to identify and manage risks independently. This can be achieved through a combination of security measures, training and guidance, and the implementation of our policies. In furtherance of our duty to safeguard staff and learners, the Trust will aim to ensure that staff and children/young people stay safe online.

Online safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences. The online world is developing rapidly and most of our children/young people have access to devices which enable them to connect to the internet, take images, videos and communicate with others. The use of these exciting and innovative tools in our academies and at home has been shown to raise educational standards and promote the achievement of children/young people. However, the use of these new technologies can put users at risk. As stated previously, the breadth of issues within online safeguarding is considerable, Our approach to online safety is based on addressing the following categories of risk:

The 4 key categories of risk

- **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 the user 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 or semi-nudes and/or pornography), sharing other explicit images and online bullying
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Many of these risks reflect situations in the offline world so it is essential that this Online Safeguarding Policy is used in conjunction with other policies including the Trust Safeguarding and Child Protection policies.

This policy applies to all members of the Trust community including staff, learners, Trustees and visitors who have access to the Trust IT systems, both on the premises and remotely. Any user of Trust IT systems must adhere to the current age-appropriate Acceptable Use Agreement.

2. Aims

Our Trust Aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and trustees
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole academy and trust community in its use of technology, including mobile and smart technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

3. 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 Academies on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study and complies with our funding agreement and articles of association.

4. Roles and Responsibilities

4.1 Trustees

The board of Trustees has overall responsibility for monitoring this policy and holding the Trust Executive Team to account for its implementation.

The board of Trustees will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding leads (DSL).

The Trustee who oversees online safety is Alison Warner

All Trustees will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms of the Trusts Acceptable Use Policy

- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse 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.

4.2 The Trust Executive Team

The Trust Executive Team has responsibility for monitoring the implementation of this policy across Brigantia Learning Trust Academies and holding individual Principals to account for its implementation within their organisation.

The Trust Executive Team will:

- Make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure all staff understand their expectations, roles and responsibilities around filtering and monitoring.
- Ensure all staff receive regular online safety updates as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.
- Ensure each academy teaches pupils how to keep themselves and others safe, including online.
- Make sure that each academy has appropriate filtering and monitoring systems in place on academy devices and networks and will regularly review their effectiveness.
- Review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:
    - Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
    - Reviewing filtering and monitoring provisions at least annually
    - Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
    - Having effective monitoring strategies in place that meet the school's safeguarding needs

4.3 The Principal

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

4.4 The Designated Safeguarding Lead

Details of the Academy's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

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

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the Academy.
- Working with the Principal, Trust Executive Team and Trustees 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 Academy devices and Academy networks
- Providing the Trust Executive Team and Trustees with assurance that filtering and monitoring systems are working effectively and reviewed regularly.
- Working with the Network manager to make sure the appropriate systems and processes are in place.
- Working with the Principal, Network manager and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the academies Child Protection and Safeguarding policy.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the academy 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 the academy to the Principal and/or the Trust Executive Team and Trustees.
- 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 The Technical Team

The technical team are responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at the academy or when accessing a Trust device outside which is not on the Trust network, including terrorist and extremist material.
- Ensuring that the academy'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 academy's ICT systems on a regular basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy's behaviour policy.

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 on acceptable use of the Trusts Acceptable Use Policy and ensuring that pupils follow the Trusts Acceptable Use Policy
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing
- Working with the DSL to ensure that any online safeguarding incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy'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 Parents/Carers

Parents/carers are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms of the Trust's Acceptable Use Policy
- Use the National Online Safety website to help keep their children safe.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Help and advice for parents/carers - Childnet International
- Parent and carers resource sheet - Childnet International

4.8 Visitors and members of the community

Visitors and members of the community who use the academy'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 off the visitors Acceptable Use Policy.

5. Educating the Brigantia Learning Trust community about online safety

5.1 Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum: Our curriculum is informed by the National curriculum in England: computing programmes of study - GOV.UK and Relationships Education, Relationships and Sex Education and Health Education guidance

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- The internet can be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health
- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- Why social media, computer games and online gaming have age restrictions and how to manage common difficulties encountered online
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private

- Where and how to report concerns and get support with issues online

In **Key Stage 3**, pupils 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

Pupils 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**, pupils 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

Across all our academies the safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Pupils will be taught age-appropriate practical cyber security skills including;

- Methods that hackers use to trick people into disclosing personal information

- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate education on safeguarding issues such as cyberbullying and the risks of online radicalisation.

5.2 Educating staff about online safety

We will:

- Provide and discuss the online safeguarding policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates. This will be done through stand-alone sessions or through drip feeding with small sessions/ daily bulletin reminders. This will cover the potential risks posed to learners (Content, Contact Conduct and Commence) as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the Academy, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues, or other members of the community.

5.3 Educating parents about online safety

Our academies will raise parents' awareness of internet safety, through the National Online Safety platform and newsletters. This policy will also be shared with parents.

Our academies 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 have any queries or concerns in relation to online safety, these should be raised in the first instance with the academies Principal and/or the DSL. Concerns or queries about this policy can be raised with the Principal.

6. Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps and forums, gaming sites and games consoles. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the academy behaviour policy and Anti Bullying Policy.)

6.1 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, including where they are a witness rather than the victim.
- Each academy will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. This will be delivered through lessons and though academy assemblies.
- 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, trustees, AAC members and volunteers receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.
- Each academy also provides information on cyber-bullying via their websites to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.
- In relation to a specific incident of cyber-bullying, academies will follow the processes set out in the academies behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the academy will use all reasonable endeavours to ensure the incident is contained.
- 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.

7. Artificial intelligence (AI)

- Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini, Co-Pilot and TeachMate AI
- The Academy 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.
- The academy will treat any use of AI to bully pupils in line with our anti-bullying and or behaviour policy.
- Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative tools such as ChatGPT, Microsoft Co-pilot and Google Gemini. Our trust recognises that AI has many uses to help staff work and pupils learn, but also poses risks to online safety.

  To ensure the online safety, of staff and students, no one is permitted to enter personal and sensitive data into generative AI tools or chatbots including those authorised by the trust. Where staff and students identify a requirement to process this type of data, with

generative AI, they must first contact the trust Senior Compliance and Operations Officer – actionline@brigantiatrust.net

8. Internet filtering and monitoring

Brigantia Learning Trust ensures that each academy has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks. Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances. Smoothwall Monitor is used by the trust across all academies. It is a human moderated digital monitoring solution. It alerts designated school staff to students suspected of becoming vulnerable based on their digital behaviours. Smoothwall Monitor is a virtual assistant that enables school staff to concentrate on supporting and educating their young people safe in the knowledge that should a suspected incident arise; they will be alerted immediately. This is a 24/7/365 service so even out of school hours, students are protected online when using a school device, however, any alerts to worrying content will be logged and acted on during the hours 8am – 4pm Monday to Friday during term time.

All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

9. Further information to support you

We work with our local safeguarding partners to ensure our students are safeguarding. We will liaise with these partners where there are safeguarding concerns and will follow their policies and procedures when needing their support. This may include referrals or seeking advice from Children's Social Care, our local Prevent team and/ or the police.

For parents the following websites could be of use:

- Samaritans: Talking to your child about self-harm and suicide content online
- NSPCC Online Safety Guides for parents
- Report harmful content at https://reportharmfulcontent.com/
- Report concerns to the NSPCC https://www.nspcc.org.uk/keeping-children-safe/online-safety/online-reporting/
- Thinkuknow- how to help your children get the most out of the internet.
- Further guidance shared by the DfE can be accessed here

For students the following websites could be of use:

- Mind- mental health support
- Togetherall- online community accessible 24/7
- Shout- a free text service available 24 hours a day. You can start a conversation by texting Shout to 85258
- Samaritans' self-help app
- Kooth is an online mental wellbeing community for young person
- Report harmful content at https://reportharmfulcontent.com/child/
- Report concerns to the NSPCC https://www.nspcc.org.uk/keeping-children-safe/online-safety/online-reporting/

For all staff and volunteers it is useful to be aware of the resources available to staff and students so that you can signpost them as required. In addition, the following resources could be of use:

UK Safer Internet Safety- teacher guides and resources

https://www.internetmatters.org/schools-esafety/

https://www.gov.uk/government/publications/teaching-online-safety-in-schools/teaching-online-safety-in-schools

Policies/ guidance to be read and understood alongside our online safety policy:

- Child Protection and Safeguarding policy.
- Behaviour policy.
- Staff Code of Conduct inc. acceptable use of technology in the staff behaviour policy/ code of conduct.
- Anti-bullying Policy including cyberbullying
- The Prevent Duty and The Prevent duty: an introduction for those with safeguarding responsibilities
- Meeting digital and technology in schools and colleges (DfE)