Online Safety Policy

Policy Owner	**Sophie Evitts**
Role	**Head of Site**
Date issued	**November 2024**
Chair of Governors Signature	
Date and Minute Number	**10th February 2025 - 1066**

Next review date	Reviewed Date	Reviewed By	Changes made to the policy	Date and Minute number	Chair of Governors signature
November 2025			Policy owner name change. New logo added. Across two sites added. Aged 3-19 added.		
April 27	10/04/26	Sophie Evitts	Please see highlights	20/04/2026 - 2021	

Table of Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors across two sites.
- Identify and support groups of pupils aged 3-19 that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships, health 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 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, acknowledging pupils will not be able to access its full content, and therefore use bespoke computing curriculum appropriate to the development needs and stage of pupils.

All online safety incidents are recorded on My Concern in line with the Child Protection and Safeguarding Policy.

3. Roles and responsibilities

3.1 The governing board

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

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

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The 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 school 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 governor who oversees online safety is Traci Good.

All governors will:

- Ensure 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 online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

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

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) 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 school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

- Working with the headteacher 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 school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT 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 school's child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or 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.

3.4 The ICT/ Network manager

The school has a named Filtering and Monitoring Lead (ICT/Network Manager) who works closely with the DSL. Any safeguarding concerns identified through monitoring systems are escalated immediately to the DSL and logged in line with safeguarding procedures.

The ICT/ Network manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis and reporting to DSLs and governors
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) 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

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- 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 logging concerns on My Concern or the helpdesk@
- Following the correct procedures by contacting the IT/ Network Manager 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 5) 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'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

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

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the computing, personal development and preparation for adulthood curriculum approach. See the long term plan for coverage for stage and age of pupils.

Online safety is taught through the Special agents online safety curriculum; designed specifically to develop digital resilience and safe online practice for young people with SEND.

Digital Resilience and Online Safety

In addition to the content in the online safety policy and acceptable use of the internet and electronic communication policy, pupils have embedded online safety lessons linked to their PLIs to increase their digital resilience.

Early use of digital technology has been shown to improve language skills and promote children's social development and creativity. However, the risks to personal safety and inappropriate content are a growing concern and constantly changing. Pupils have vital information to the digital world and as a result we hold regular pupil voice sessions to learn about the latest trends, interests, concerns and plan meaningful pupil-led initiatives to support the school community.

Pupils all have a school computer account. These are used on laptops. Accounts are set up as:

Username – first initial surname (and for Microsoft logins the same approach with @brackenfield.derbyshire.sch.uk after the name)
Password – A Password protected Master File is stored on Microsoft Teams enabling a move away from generic passwords for all pupils to a password tailored to each pupil (set to **not** ask to be changed on first log in) – All staff have access to the file in order to support pupils. The password reflects recommended password requirements having elements of upper and lower case letters, numbers and special characters.

Pupils save their work on Teams/Sharepoint, reflecting the changing way that documents are saved and shared in today's modern, online world.

See the handbook for reporting processes for pupils: **Pupil Policy handbook - updated 100724.docx**

iVengers Special Agents

Pupils with SEND struggle to transfer skills learnt in the classroom to the outside world. Often pupils with SEND can verbalise a rule and recite how to stay safe but fail to notice the risks when they occur in the moment. Pupils with SEND are often captivated by devices and technology, with skills which surpass their generalised ability to access the world around them. This too causes additional risk and vulnerability as pupils are exposed to potential risks by chance. Pupils with SEND maybe developmentally and cognitively impaired, however more often than not, their online experience is similar to their neuro-typical peers. Special Agents creates an open dialogue with pupils, staff and parents about what pupils are doing online and how to do it safely.

Special Agents are focused on immersive learning creating a positive digital world common language embedded in the school community.

The main objectives are:

- To create a digital persona
- To demonstrate how digital life should be
- Facilitate positive online experiences
- To open up access to the positive digital world
- Facilitate in the moment problems leading to problem solving
- Learn the steps to access content we want
- To support peers with learning

Creating a Digital World and Immersive Environment

At Brackenfield, online safety replicates the curriculum models. We immerse pupils in online activity which is accessible to them supporting progress through motivators, strengths and needs. We promote positive online experiences to enrich pupils' opportunities in a digital world.

You Tube is the most common online experience in school. It starts at home, families use You Tube to motivate even the most complex SEN needs at home and support regulation.

Within the informal curriculum, pupils have videos embedded into routines. Videos are shared with home and chosen to reflect pupil interests. Our immersive classroom is interactive, along with our sensory rooms and portable sensory projector- promoting cause and effect opportunities. iPads are used to take photos to support communication in the moment- to improve clarity of messages, to support pupil understanding and decision making.

In the semi formal curriculum, pupils also use videos to listen to stories, learn new signing, make and watch videos of themselves and their friends as well as help structure their day. Pupils have access to iPads with games focused on early maths and literacy skills- as well as early communication. Pupils continue to use YouTube but for enjoyment purposes- this ever growing sense of independence on an iPad has huge impact on confidence. Pupils explore desktop devices to draw, find photos of interest, play games and communicate with peers.

All pupils have Teams accounts. These are used for video calls with pupils who are at home, if they wish to engage with lessons in school. Classes call other classes within school too. Pupils can access Teams outside of school. This platform is promoted for pupils to message each other in the chat function. This is monitored by staff and when problems arise can be addressed straight away in the classroom. Pupils use Microsoft applications as part of the independent living curriculum, on laptops and iPads. This not only teaches them the skills to use these but opens up accessibility from home as well. Visually impaired pupils are taught the steps to use audio features and increase font size etc. Pupils are taught the importance of keeping passwords safe and changing them. This is a hard but necessary life lesson- knowing how to reset your password.

We host virtual enrichments- including both primary and secondary aged pupils. This happens after school via Teams. Pupils have a focus for the session, it might be games or an arts and crafts club. This is chosen through pupil voice. School supply arts materials for pupils to take home and complete the project over Teams. Staff are also involved as role models, to model expectations replicating what we do in school.

Pupils use devices to take their own photos to support recalling information, sequencing, comprehension and communication. Pupils are given problems to solve to teach online safety rules, in contexts they access, to ensure safety is transferable and not just a learned script which is not applied.

In the formal curriculum, pupils are equally as immersed as all the other pupils across school. In this curriculum model it is very clear how pupils can navigate and manipulate the digital world with low levels of literacy and numeracy. We are keen to empower our students to be confident in a digital world- where usually they would feel vulnerable and different. Pupils take part in virtual enrichment, daily communication between friendship groups on platforms set up by school. By introducing Teams, pupils have moved away from games like Roblox to communicate. This has reduced the risk online as Teams is secure and managed by school. By promoting positive online activity and celebrating it- emailing opportunities to staff and peers, blogger style videos, onsite games consoles, iPads and curriculum apps- pupils have learned online experience to transfer at home. We continue to remind of rules and risks applicable to the activities the pupils do.

5. Educating parents/carers about online safety

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

Online safety will also be covered during parents' evenings.

The school 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 headteacher and/or the DSL.

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

6. Cyber-bullying

6.1 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 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.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Where appropriate, class teachers will discuss cyber-bullying.

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 pupils, as part of safeguarding training (see section 11 for more detail).

The school 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 school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school 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.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school 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 pupils and staff. If the search is not urgent, they will seek advice from the Headteacher or a DSL
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it

- Seek the pupil'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 school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the DSL, Headteacher and/ or senior leaders to decide on 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 pupil 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 pupils 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 / searches and confiscation policy

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

6.4 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 Bard.

Brackenfield SEND School 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.

AI tools may be used to support learning, communication and accessibility where appropriate, particularly for pupils with SEND. Staff must ensure that personal data is not entered into AI systems and that AI use aligns with GDPR, data protection policies and safeguarding expectations.

Brackenfield SEND School will treat any use of AI to bully pupils in line with our 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 the school.

7. Acceptable use of the internet in school

All pupils, parents/carers, 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 and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in the Acceptable Use of IT Policy.

8. Pupils using mobile devices and SMART watches in school

Pupils may bring mobile devices and SMART watches into school, but are not permitted to use them unless directed to do so as part of life skills lessons.

Any use of mobile devices and SMART watches in school by pupils must be in line with the acceptable use agreement.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

See more details in the mobiles phone policy.

9. 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) or, on iPad a 6 digit passcode.
- 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 locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software where appropriate
- Keeping operating systems up to date by always installing the latest updates or requesting this from IT

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in the acceptable use agreement.

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 IT/ Network Manager.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and individual behaviour support plans/ risk assessments. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Online sexual harassment and abuse are treated as safeguarding concerns and responded to in line with the Child Protection and Safeguarding Policy, including child-on-child abuse procedures.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures / staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that 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 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 up the risks
- 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/ 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 policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the Lead DSL. At every review, the policy will be shared with the governing board. 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.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Mobile phones policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy including acceptable use agreement