



## Online Safety Policy

<b>Committee</b>	Trust Board
<b>Author</b>	Danielle Bennett
<b>Version</b>	1.0
<b>Approved on</b>	16 <sup>th</sup> October 2023
<b>Signature</b>	R Hover
<b>New Review date</b>	October 2024

**Review Procedures**

This Policy will be reviewed regularly and revised as necessary. Any amendments required to be made to the Policy as a result of a review will be presented to the relevant committee for approval.

Document / revision no.	Date	Status / Amendment	Approved by



## CONTENTS

1. Aims	4
2. Legislation and guidance	4
3. Roles and responsibilities	5
3.1 The Safeguarding & Health & Safety Committee	5
3.2 The headteachers	6
3.3 The designated safeguarding leads	6
3.4 The ICT Technician (SNS)	7
3.5 All staff and volunteers	7
3.6 Parents/carers	8
3.7 Visitors and members of the community	8
4. Educating pupils about online safety	8
5. Educating parents/carers about online safety	9
6. Cyber-bullying	9
6.1 Definition	9
6.2 Preventing and addressing cyber-bullying	9
6.3 Examining electronic devices	10
6.4 Artificial intelligence (AI)	11
7. Acceptable use of the internet in school	12
8. Pupils using mobile devices in school	12
9. Staff using work devices outside school	12
10. How the school will respond to issues of misuse	13
11. Training	13
12. Monitoring arrangements	14

## 1. Aims

### **Our Trust aims to:**

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- 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 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 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.

### **3. Roles and responsibilities**

#### **3.1 The Safeguarding & Health & Safety Committee**

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

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

The committee 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 committee 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 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.

All committee members will:

- Ensure they have read and understand this policy
- Agree to adhere to the terms on acceptable use of the Trust's ICT systems and the internet

- Ensure that online safety is a running and interrelated theme while devising and implementing their 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 headteachers

The headteachers are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the schools.

### 3.3 The designated safeguarding leads

Details of the schools' designated safeguarding leads (DSL) deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSLs takes lead responsibility for online safety in schools, in particular:

- Supporting the headteachers in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteachers and the Safeguarding & Health & Safety 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 devices and schools networks
- Working with the SNS (ICT technicians) to make sure the appropriate systems and processes are in place
- Working with the headteachers, ICT technicians 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 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 Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteachers and the Safeguarding & Health & Safety Committee.
- 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 Technician (SNS)

The ICT technician 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 schools' 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 weekly 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 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
- Adhering to the Trust's acceptable use policy when using the Trust's ICT systems and the internet and ensuring that pupils follow the Trusts' policy on acceptable use.
- Knowing that the DSLs are 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 a DSL.
- Following the correct procedures by obtaining the Headteachers' permission if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSLs 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'

This list is not intended to be exhaustive.

### 3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteachers of any concerns or queries regarding this policy
- Ensure their child understands what is considered acceptable use of their schools ICT systems.

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 schools' ICT systems or internet will be made aware of this policy and the acceptable use policy, when relevant, and expected to read and follow it.

## 4. Educating pupils about online safety

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

**All** schools have to teach:

- [Relationships education and health education](#) in primary schools

In **Key Stage (KS) 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 (KS) 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:

- 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
- 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 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.

### **5. Educating parents/carers about online safety**

The schools will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our websites. 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 their headteacher and/or the DSL.

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

### **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. 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).

In relation to a specific incident of cyber-bullying, the schools will follow the processes set out in the schools' behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the schools 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 their Headteacher.
- 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 headteacher 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](#)
- The Behaviour 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.

Inspira Academy Trust 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.

Inspira Academy Trust will treat any use of AI to bully pupils 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 the Trust.

### **7. Acceptable use of the internet in school**

All pupils, parents/carers, staff, volunteers and governors are expected to adhere to the this policy and the Trust's acceptable use policy. Visitors will be expected to read and agree to the Trust's policies on acceptable use if relevant.

Use of the schools' 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.

For more information please see the Acceptable use Policy.

### **8. Pupils using mobile devices in school**

Pupils in Years 5 & 6 may bring mobile devices into school, but must hand them into their class teacher at the start of the day and collect at the end of the day. Pupils in other year groups must obtain permission from the Headteachers if they need to bring a mobile device into school.

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

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.

### **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 with strong passwords.
- 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
- Keeping operating systems up to date by always installing the latest updates

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

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 SNS technician.

## **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 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 Trust'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 code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The Trust 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 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 policy.

## **12. Monitoring arrangements**

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

This policy will be reviewed every year by the Safeguarding & Health & Safety Committee. At every review, the policy committee. 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
- Behaviour policy
- Staff Code of Conduct
- Data protection policy and privacy notices
- Complaints procedure
- Acceptable use policy