ONLINE SAFETY POLICY

Version	2.0
Approving Body	Trust Board
Date ratified	September 2025
Date issued	September 2025
Review date	3 yearly
Owner	Trust CEO
Applies to	All Trust Schools, all Trust staff

Version	Date	Reason
1.0	July 2022	To establish a trust-wide policy
2.0	September 2025	Reviewed as part of the review cycle

Contents

1. Aims

Initio Learning Trust aims to:

- Have robust processes in place to ensure the online safety of pupils.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole trust 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, anti-Semitism, radicalisation and extremism and misinformation, disinformation (including fake news) and conspiracy theories.

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

2. 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

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 Initio Learning Trust

The Trust has overall responsibility for monitoring the implementation of this policy.

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

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, digital technology leader and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the Safeguarding and Child protection policy
- Ensuring that any online safety incidents are logged on MyConcern and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are logged on My Concern and dealt with appropriately in line with the school behaviour and Anti-bullying 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 Local School Committee

This list is not intended to be exhaustive.

3.4 The Director of Operations/Head of IT

The Director of Operations takes the lead on systems to support this policy:

- Putting in place an appropriate filtering and monitoring systems for all Trust owned devices and those not owned by the trust whilst on trust premises. Such systems are reviewed and updated on a regular basis to assess effectiveness and ensure the likelihood of pupils accessing potentially harmful and inappropriate content is reduced as far as is practical.
- Ensuring that the Trust ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- That headteachers and DSL's can access reports on use of the Trust ICT systems that may represent a safeguarding concern.

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 and Implementing this policy consistently
- Adhering to the terms of the Trust ICT Responsible Use policy when using Trust 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 or incidents of cyber-bullying are logged on My Concern and dealt with appropriately in line with this policy and 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

Parents 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

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

What are the issues? – UK Safer Internet Centre

Hot topics – Childnet International

Parent resource sheet – Childnet International

Healthy relationships – Disrespect Nobody

Helping parents keep their children safe online - Internet Matters

-

3.7 Visitors and members of the community

Visitors and members of the community who use the Trust ICT systems will be made aware of this policy and expected to read and follow it. They will be expected to adhere to the Trust ICT Responsible use policy.

4. Educating pupils about online safety

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

All schools have to teach:

Relationships Education, Relationships and Sex Education (RSE) and Health Education

See appendix A for details of educating pupils about online safety.

5. Educating parents about online safety

The Trust and its schools will raise parents' awareness of internet safety in letters or other communications. 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.

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 one person or group by another person or group, where the relationship involves an imbalance of power.

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 Trust and its schools 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, Local School Committee members, volunteers and Trustees (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying 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, the school will follow the processes set out in the school behaviour and anti-bullying 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 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.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

Cause harm, and/or

Disrupt teaching, and/or

Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

Delete that material, or

Retain it as evidence (of a criminal offence or a breach of school discipline), and/or

Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

The DfE's latest guidance on screening, searching and confiscation

UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

The Trust and school's COVID-19 risk assessment

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

7. Acceptable use of the internet in school

All employees, Trustees, Local School Committee members, volunteers, visitors and any contractors using our ICT facilities should follow the ICT Responsible Use policy.

For pupils and students, expectations are set out in the Acceptable Use Agreements: see Appendix B for EYFS/KS1 and Appendix C for KS2/3/4

We will monitor internet use and compliance with these policies and agreements .

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but they are not permitted to be used on school site.

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

9. How the school will respond to issues of misuse

Where a pupil misuses the Trust or its schools ICT systems or internet, we will follow the procedures set out in our Behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

The Trust and its schools will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

10. 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

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.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

11. Monitoring arrangements

The Trust and its schools will monitor behaviour and safeguarding issues related to online safety through My Concern software.

12. Links with other policies

This online safety policy is linked to our:

Safeguarding and child protection policy
Behaviour policy
Code of Conduct
Data protection policy and privacy notices
Complaints procedure
ICT Responsible use policy
Child on Child abuse policy
Youth Involved imagery Policy

Appendix A

Educating Pupils about Online Safety.

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:

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

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 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.

Appendix B

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers	
Name of pupil:	
When I use the school's ICT systems and get onto the internet in school I will: · Ask a teacher or adult if I can do so before using them · Only use websites that a teacher or adult has told me or allowed me to use · Tell my teacher immediately if: o I click on a website by mistake o I receive messages from people I don't know o I find anything that may upset or harm me or my friends · Use school computers for school work only · Be kind to others and not upset or be rude to them · Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly · Only use the username and password I have been given · Try my hardest to remember my username and password · Never share my password with anyone, including my friends. · Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer · Save my work on the school network · Check with my teacher before I print anything · Log off or shut down a computer when I have finished using it **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix C

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy **When I use the school's ICT systemsand get onto the internet in school I will:** · Always use the school's ICT systems and the internet responsibly and for educational purposes only · Only use them when a teacher is present, or with a teacher's permission · Keep my username and passwords safe and not share these with others · Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer · Tell a teacher immediately if I find any material which might upset, distress or harm me or others · Always log off or shut down a computer when I'm finished working on it **I will not:** · Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity · Open any attachments in emails, or follow any links in emails, without first checking with a teacher · Use any inappropriate language when communicating online, including in emails · Log in to the school's network using someone else's details · Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** · I will not use my personal device while on the school site. **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**