Online Safety Policy

Approved by:	Governing Body	Date: July 25
Last reviewed on:	July 2025	
Next review due by:	July 2026	

Contents

1. Aims

ISP school aims to:

Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors. We use smoothwall as a secure mechanism to safeguard our school community. Smoothwall notifies the Headteacher if there is a breech or concern during the school day and any incidents can be addressed immediately.

Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology

Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education 2024, 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 cyberbullying 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.

3. Roles and responsibilities

3.1 The governing board

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

The governing board will discuss online safety with the Head Teacher and monitor online safety concerns logged via My Concern as provided by the designated safeguarding lead (DSL).

All governors will:

Ensure that they have read and understand this policy

Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

3.2 The Head Teacher

The Head Teacher 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

Our DSL is: Deputy Head Teacher – Kerry Keeble

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

- Supporting the Head Teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Head Teacher, ICT lead and other staff, as necessary, to address any online safety issues or incidents
- 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 Head Teacher and/or governing board

3.4 ICT – Polaris IT in conjunction with the HT and ICT lead.

The Polaris IT/HT and ICT lead 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 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 monthly 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 (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

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)
- Working with the DSL to ensure that any online safety incidents are logged on My Concern 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

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Head Teacher 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)
- 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 factsheet - Childnet International Healthy relationships – Disrespect Nobody

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 curriculum:

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 KS1**, 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
- 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 **KS3/4,** 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

The safe use of social media and the internet will also be covered in other subjects where relevant.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or Class Dojo. 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 Head Teacher and/or the DSL.

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

6. Artificial Intelligence (AI)

Polaris is committed to continuously monitoring progress in the field of AI and adapting our approach in an appropriate and proportionate way as new capabilities emerge.

We will adopt a flexible approach to this fast developing technology whilst safely balancing the opportunities and risks and adhering to best practice and government standards.

The UK Government has taken a "pro-innovation" approach to AI, which means that it is not planning any new legislation or regulation around its use and as such Polaris is providing this statement to make our position clear on the use of AI.

Definition

Artificial intelligence (AI) is the capability of a computer system to mimic human cognitive functions such as learning and problem-solving. Through AI, a computer system uses maths and logic to simulate the reasoning that people use to learn from new information and make decisions. AI is an umbrella term that encompasses a wide variety of technologies, including machine learning, deep learning, and natural language processing (NLP). AI is already in use in daily life such as satnavs and Alexa/Siri.

AI is used operationally in business to automate tasks traditionally done by humans, including customer service, enquiry generation, data analysis and marketing activities and as such is used by some service areas across the Polaris community effectively for business & marketing purposes.

Natural Language Processing (NLP) such as ChatGPT

In other service areas of Polaris, individuals who provide services within the community and are responsible for record-keeping have the option to use text-based applications like ChatGPT. This is an area that requires more consideration.

Copyright Polaris

The inspectorate will consider a provider's use of AI by the effect it has on the criteria set out in existing inspection frameworks. They will assess AI's impact on children as part of the wider inspection and regulatory processes. Ofsted, for example, support the use of AI by providers where it improves the care of children. See Ofsted's approach to artificial intelligence (AI) - GOV.UK.

The re-writing of notes/records or comments using AI could raise questions about the authenticity of the records as to whether they truly reflect the professional's perspective. Care records should accurately reflect the observations and professional judgement of the practitioner/worker, not the AI's reinterpretation.

Summarising notes using AI could miss the subtle emotional and situational cues that AI may fail to capture and could result in oversimplified or over exaggerated summaries. AI

could misinterpret the context or intent behind a practitioner/worker's notes leading to errors in the re-written version.

Polaris accepts that AI is a useful tool for editing text but should not be used to fill in gaps or add content that is additional to the original notes. Care must be exercised if using AI to reword any notes or records, ensuring that you proofread before saving and are confident that it still accurately reflects the intent and findings of your original comments and observations.

This stance is echoed by NAFP in their article Artificial intelligence and foster care | Nationwide Association of Fostering Providers which states:

'AI undeniably possesses remarkable capabilities. It can process information faster than a human can and excels at specific tasks with astonishing precision. However, there are also many things it cannot do. Most notably, it is not human! We have created artificial intelligence not artificial empathy, so it cannot replace the human approach which must sit at the centre of the children's care sector.

Best Practice re GDPR

⬚ If you're using ChatGPT or any other AI language model through a platform with privacy settings, review your account settings for options related to 'data collection' or 'learning'. For ChatGPT, this can be found under 'data controls' in the settings, where you can simply deselect the relevant option.

⬚ Avoid entering sensitive or personally identifiable information into ChatGPT or any other AI language model, as they are not designed to ensure the security or privacy of confidential data.

⬚ Before uploading or pasting data into ChatGPT or any other AI model, anonymise it as much as possible. After processing, add any personal details back into your recording system.

If you are using AI tools in the course of your work, this should be transparent and in agreement with your line manager. If you are in any doubt about whether the use of AI based tools is appropriate or need support or guidance, please consult your line manager for advice.

7. Cyber-bullying

7.1 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. (See also the school Behaviour Policy.)

7.2 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. Class teachers will discuss cyber-bullying with their classes.

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 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 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.

7.3 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

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation and the 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 school complaints procedure.

8 Online Hate

Online hate content, directed towards or posted by, specific members of the community will not be tolerated at ISP School Teynham and will be responded to in line with existing policies, including anti-bullying and behaviour. All members of the community will be advised to report online hate in accordance with relevant policies and procedures. The Police will be contacted if a criminal offence is suspected. If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding Service and/or Kent Police.

9 Online Radicalisation and Extremism

We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site. If we are concerned that November 2022 27 Theeducationpeople.org a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy. If we are concerned that member of staff may be at risk of radicalisation online, the headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

8. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). 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.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

iPads have added functionality provided by Polaris IT department. This includes individual logins for students and the Classroom app available to teachers via teacher iPads. Classroom allows staff to lock a specific student iPad if it is being misused.

9. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during the school day. The mobile phones will be kept in the class teacher's lockable draw or in

reception.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1).

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.

10.   Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Updating anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

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 DSL and the ICT Team.

11.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. 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 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 which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12.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).

The DSL DDSL 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.

13. Monitoring arrangements

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

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

14. Links with other policies

This online safety policy is linked to our:

Child protection and safeguarding policy

Behaviour Policy

Staff disciplinary procedures

Data protection policy and privacy notices

Complaints procedure

ICT and internet acceptable use policy
Mobile phone policy

Appendix 1: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/foster Foster Foster Parents)

Online Safety School Agreement

Pupil

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's laptops, iPads and the internet responsibly and for my lessons

- Only use them when a teacher or PEG 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/foster parent

- Tell a teacher or a PEG immediately if I find any material which might upset or harm 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 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 on Class Dojo
- Log in to the school's network using someone else's details

If I bring a personal mobile phone or other personal electronic device into school:
- I will not use it during the school day, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online
- I agree that the school will monitor what I do online and that there will be consequences if I don't follow the rules.

Signed: ……………………………………………………………………………………………..
Date:
Pupil: …………………………………………………………………………………………….

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)

Use them in any way which could harm the school's reputation

Access social networking sites or chat rooms

Use any improper language when communicating online, including in emails or other messaging services

Install any unauthorised software, or connect unauthorised hardware or devices to the school's network

Share my password with others or log in to the school's network using someone else's details

Take photographs of pupils without checking with teachers first

Share confidential information about the school, its pupils or staff, or other members of the community

Access, modify or share data I'm not authorised to access, modify or share

Promote private businesses, unless that business is directly related to the school

---

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT Team know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

| **Signed (staff member/governor/volunteer/visitor):** | **Date:** |

Appendix 3: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

1	November 2022	
2	May 2023	M Jenkinson
3	July 2025	M Jenkinson