# IT and Online Safety Policy incorporating Acceptable Use Policy 2024-2025

| | | |
|---|---|---|
| **Approved by:** | Academy Committee | **Date:** 23rd September 2024 |
| **Last reviewed on:** | September 2024 | |
| **Next review due by:** | September 2025 | |

# Contents



## Aims

Our school aims to:

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

### 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

## 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.

Meeting digital and technology standards in schools and colleges March 2023

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.

This policy complies with our funding agreement and articles of association.

## Roles and responsibilities

### The Academy committee

The Academy committee has overall responsibility for monitoring this policy and holding the head of school to account for its implementation.

The Academy committee will co-ordinate meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The Academy committee has overall strategic responsibility for filtering and monitoring in school. It 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 Academy 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 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.

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 IT systems and the internet (appendix 2)

## The Headteacher

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

## The designated safeguarding lead and Line Manager for IT

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy.

The DSL and Line Manager for IT take 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.

## The Trust Network manager

The Trust network Manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Monitoring the school's IT 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 and reported; radicalisation will require

an immediate alert; others will be included in a half termly review

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Ensuring that inappropriate keywords in emails are flagged and shared in an email box called “incidents”

This list is not intended to be exhaustive.

### 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
- 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 making an appropriate report on CPOMs
- Agreeing and adhering to the terms on acceptable use of the school’s IT systems and the internet (appendix 2), and ensuring that students follow the school’s terms on acceptable use (appendix 1)
- Working with the DSL 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

This list is not intended to be exhaustive.

### Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the Head of School of any concerns or queries regarding this policy
- Ensure students have read, understood and agreed to the terms on acceptable use of the school’s IT systems and internet (appendix 1)

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

### Visitors and members of the community

Visitors and members of the community who use the school’s IT 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 2).

## Educating students about online safety

Students will be taught about online safety as part of the curriculum.

In **Year 7 & 8,** students 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

In **Year 9,** students will have an internet safety unit as part of the tutor programme and in their PD lesson. In **Year 10 and 11** students 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
- Managing sexual pressure online

The safe use of social media and the internet will also be covered in other subjects where relevant but in particular Personal Development lessons.

The school will use assemblies to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

## Educating parents/carers about online safety

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

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the assistant headteacher responsible for IT and/or the DSL.

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

## Cyber-bullying

### 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)

### Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

We highlight to parents/carers that age limits apply to social media applications and these age limits are put in place for a reason. We encourage youngsters to only engage with social media when they are an appropriate age and if parents/carers are confident that they are mature enough to do so. We advise parents/carers to monitor the use of social media and be aware of what children are posting.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Heads of Year and tutors will discuss cyber-bullying with their year groups/tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber- bullying. This includes Personal Development education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training.

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 students, 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 agencies if it is deemed necessary to do so.

### Examining electronic devices

The Head of School or staff authorised by them, 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 Head of School / DLS / appropriate staff member
- 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

The Senior Leadership Team 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 staff member in conjunction with the DSL / Head of School / other member of the senior leadership team] 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

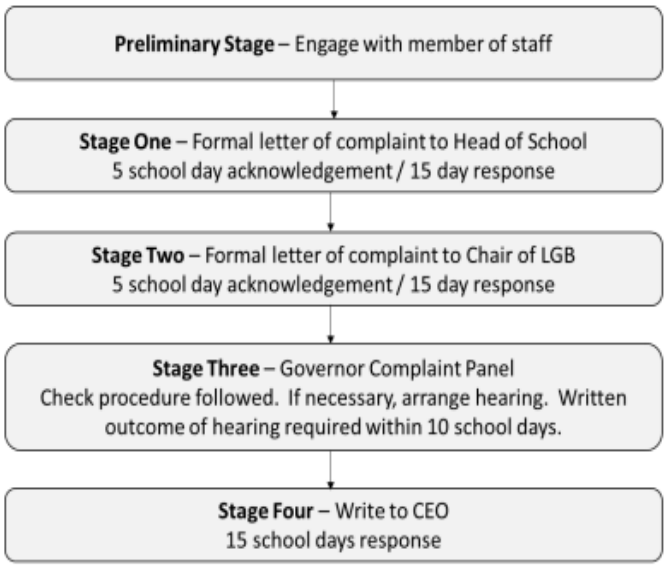
and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

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

**School Level Complaint**




**Trust Level Complaint**

A school complaint does not become a trust complaint


## 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.

HISP Trust and Thornden 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.

HISP Trust and Thornden School will treat any use of AI to bully pupils in line with our anti-bullying/behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed.

## Acceptable use of the internet in school

All students, parents, carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet (appendices 1 and 2). 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.

Fortigate monitors the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. The school uses a combination of Fortigate and Netsweeper to help

ensure acceptable internet usage. Netsweeper provides web content filtering, that by using the Internet Watch Foundation (IWF) Block List & Image Hash List and the Home Office Terrorism Block List, protects staff and students from content that is not suitable for an education setting. This provision, supplied by the schools ISP (Talk Straight - Schools Broadband) and supported by the schools IT Team, helps keep the school compliant with Keeping Children Safe in Education guidance.

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

## Students using mobile devices in school

Students may bring mobile devices into school but are not permitted to use them during the school day. This includes:

a. Lessons & tutor time (unless specifically directed to do so by their teacher)

b. Break or lunch time

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

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

## Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and passphrase-protected, and that they do not share their passphrase with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the Trust Network Manager.

## Staff using their own devices in school

Staff must not use the device in any way which would violate the school's terms of acceptable use.

Staff must ensure that their own device is secure and passphrase-protected, and that they do not share their passphrase with others. They must take all reasonable steps to ensure the security of any Thornden data and report any breaches as per the GDPR policy.

If staff have any concerns over the security of their own device, they must seek advice from the Trust Network manager.

Own devices used must be inspected by the IT team when employment has been terminated so to remove any school licenced products/school data.

## How the school will respond to issues of misuse

Where a student misuses the school's IT systems or internet, we will follow the procedures set out in the behaviour policy. 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 IT 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. 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.

## 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 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.

## Monitoring arrangements

Any behaviour and safeguarding issues related to online safety will be logged as part of the school system.

This policy will be reviewed annually and at every review, the policy will be shared with the Academy committee.

## Links with other policies

This online safety policy is linked to our:

a. Child protection and safeguarding policy
b. Behaviour policy
c. Staff disciplinary procedures
d. Data protection policy and privacy notices
e. Complaints procedure

## Appendix 1: Student Acceptable Use Policy

I understand that I must use school IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users.

When using my personal device connected to the school Wi-Fi, I will abide by the same rules as if I was using a school device.

### I will not:

- access, remove or write files to or from any area of the network other than my designated user space unless otherwise authorised;
- allow any other person to use my log-in username and password;
- interfere with or take any action which is liable to damage the network hardware or software.
- attempt to access or download from Internet web sites where the material is likely to be unsuitable.
- send e-mails that are obscene, derogatory or liable to cause offence.
- take or distribute images of anyone without their permission.

### I recognise that I must not try and damage the school network but will:

- immediately report any damage or faults involving equipment or software, however this may have happened.
- not install or attempt to install programs of any type on a machine, or store programs on a computer, nor will I try to alter computer settings.
- not attempt to use chat or social media sites.
- not attempt to forward SPAM or chain mail using the school network.

I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

I understand that if I fail to comply with this Acceptable Use Policy Agreement, appropriate intervention will follow.

PRINT NAME: ……..

SIGNED: ……

DATE: ……

# Appendix 2: Staff Acceptable Use Policy

## The purpose of this agreement is to:

Outline the guiding principles for all members of staff regarding the use of IT.

Safeguard and protect staff and help them to work safely and responsibly whilst using the school's IT systems.

## For my own professional and personal safety:

- I understand that the school will monitor my use of the school's IT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school IT systems (e.g. school laptops, email, Thornden Cloud etc.) out of school.
- I understand that the school IT systems are intended for educational use and will use them in a professional manner.
- I will not allow any other person to use my log-in username and password, nor will I try to use any other person's.
- I will not interfere with or take any action which is liable to damage the network hardware or software.
- I will report any unpleasant material or correspondence sent to me to IT Support.
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will use all aspects of the school IT system and communicate with others in a professional manner.
- I will adhere to the Safeguarding and Child Protection Policy and the HISP Staff Code of Conduct regarding my use of chat and social networking sites.
- If the data on any device is breached, I must report this immediately to IT Support.
- I will ensure that my school loaned equipment is protected by up-to-date anti-virus software and is free from viruses. If a virus is detected this must be reported to IT Support immediately.
- When I use my personal handheld/external devices in school, I will follow the rules set out in this agreement, in the same way as if I am using school equipment.
- I understand that data protection policies require that any staff or students' data to which I have access (both in school and out of school) will be kept private and confidential.
- Use of personal devices (e.g. mobile phones) used to access school data such as email must be password protected. Please ensure IT Support is informed if your device is lost or stolen.
- All devices must be locked when left unattended.
- Any USB stick or external hard drive must be encrypted if it contains personal data.
- I will return any school devices upon termination of my employment at Thornden School.
- I understand that my accounts will be disabled, and I will be unable to access them after my termination date.
- I should ensure that I have permission to use the original work of others in my own work and it is my responsibility to understand and comply with current copyright legislation.

I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to the Academy Committee, and in the event of illegal activities the involvement of the police.

PRINT NAME: ……

SIGNED: ……

DATE: ……