IT and Online Safety Policy incorporating Acceptable Use Policy

Approved by:	Academy Committee	**Date:** 30th September 2026
Last reviewed on:	September 2026	
Next review due by:	September 2027	

Contents

Aims 2
Legislation and guidance 3
Roles and responsibilities 3
Educating students about online safety 6
Practical Cybersecurity Skills 8
Educating parents/carers about online safety 8
Cyber-bullying 9
Artificial intelligence (AI) 11
Students using mobile devices in school 13
Staff using work devices outside school 13
Staff using their own devices in school 14
How the school will respond to issues of misuse 14
Training 14
Monitoring arrangements 15
Links with other policies 15
Appendix 1: Student Acceptable Use Policy 16
Appendix 2: Staff Acceptable Use Policy 17

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, including mobile and smart technology.
- Identify and support groups of pupils that are potentially at greater risk of harm online than others.
- 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, extreme sexual or physical violence, misinformation, disinformation and conspiracy theories.
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, other users or generative AI applications that simulate this, 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 explicit images including those generated using AI.

- **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
- Mobile phones in schools

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, the Equality Act 2010 and the Children's Wellbeing and Schools Act 2026. 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 programs.

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 headteacher 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)
- Ensure that Online Safety is a running and interrelated theme in the whole-school approach to safeguarding
- All staff receive online safety training as part of safeguarding training
- Staff understand their filtering and monitoring duties
- Staff receive updates at least annually
- Students are taught how to keep themselves safe and other safe online and that where necessary it is adapted approp
- SLT reviews the effectiveness of filtering and monitoring at least once every academic year.

The Headteacher

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

The Headteacher will ensure that robust arrangements are in place to ensure safeguarding concerns are received, monitored and acted upon without delay when the DSL is unavailable, including appropriate cover through the school's trained Deputy DSL team.

The Designated Safeguarding Lead

The Designated Safeguarding Lead (DSL) takes lead responsibility for online safety as part of the school's safeguarding arrangements.

The DSL is responsible for:

- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.
- Working with the Headteacher, Line Manager for IT, Trust Network Manager and other relevant staff to ensure that the school's filtering and monitoring arrangements meet the safeguarding needs of the school.
- Ensuring that safeguarding concerns identified through filtering and monitoring systems are responded to appropriately.
- Providing governors with assurance that filtering and monitoring systems are working effectively and are reviewed regularly.
- Managing online safety safeguarding concerns and incidents in accordance with the school's safeguarding procedures.
- Ensuring that online safety safeguarding concerns are appropriately recorded on CPOMS.
- Ensuring that incidents of cyber-bullying which raise safeguarding concerns are responded to appropriately and in accordance with the school's Behaviour Policy and safeguarding procedures.
- Ensuring that staff receive appropriate safeguarding training and updates in relation to online safety, including emerging online risks and harms.
- Liaising with other agencies and external services where necessary in relation to online safety safeguarding concerns.
- Providing appropriate reports on online safety and safeguarding to the Headteacher and/or Academy Committee.
- Contributing to the annual review of the school's online safety arrangements and risks, recognising the rapidly changing nature of technology and online harm.

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

This list is not intended to be exhaustive.

The Line Manager for IT

The Line Manager for IT has strategic oversight of the school's IT provision and works closely with the DSL, Trust Network Manager and other relevant staff to support the effective implementation of this policy.

The Line Manager for IT is responsible for:

- Supporting the Headteacher in ensuring that the IT and technical aspects of this policy are implemented consistently across the school.
- Working with the DSL and Trust Network Manager to ensure that appropriate filtering and monitoring systems are in place and support the safeguarding needs of the school.
- Maintaining an appropriate understanding of the school's filtering and monitoring arrangements and how these operate in practice.
- Working with the Trust Network Manager to ensure that **Smoothwall Cloud Filter** is appropriately deployed and maintained across all managed school and Trust devices.
- Supporting the regular review of filtering and monitoring arrangements, including the annual review of their effectiveness.
- Ensuring that technical concerns or failures relating to filtering, monitoring or IT security are addressed promptly and escalated appropriately.
- Working with the DSL to ensure that any technical information required to investigate or respond to an online safety or safeguarding concern is made available.
- Supporting the school's response to emerging technological risks and developments, including the use of artificial intelligence and other new technologies.
- Liaising with the Trust Network Manager and other Trust staff on matters relating to IT security, filtering, monitoring and the safe use of technology.
- Providing appropriate information and assurance to the Headteacher, DSL and Academy Committee regarding the school's IT systems and online safety arrangements.

The Trust Network manager

The Trust network Manager is responsible for:

- Putting in place and maintaining appropriate filtering and monitoring systems across school and Trust devices.
- Ensuring that **Smoothwall Cloud Filter** is deployed and maintained across all managed school and Trust devices so that filtering remains active both on and away from school and Trust networks.
- Ensuring that filtering and monitoring systems are reviewed and updated as appropriate and that their effectiveness is reviewed at least annually.
- Ensuring that the school's IT systems are secure and protected against viruses, malware and other cyber security threats.
- Monitoring the school's IT systems and responding appropriately to concerns or identified risks.
- Blocking access to potentially harmful, inappropriate or illegal content and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that safeguarding concerns identified through filtering and monitoring systems are reported promptly to the DSL or appropriate safeguarding staff.
- Working with the DSL and senior leaders to ensure that filtering and monitoring arrangements meet the safeguarding needs of the school and relevant DfE filtering and monitoring standards.
- Ensuring that any significant failure or concern relating to filtering and monitoring is reported promptly to the DSL and appropriate senior leaders.

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 the correct procedures if they need to bypass filtering and monitoring systems for educational purposes.
- 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.'
- 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 Headteacher 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 and by the end of Year 11 students should know about:

- rights, responsibilities and expectations of behaviour online;
- privacy and location settings;

- differences between public and private online spaces;
- fake social media accounts;
- AI-generated content;
- exaggerated/idealised online identities;
- risks of distributing personal material;
- the law relating to sharing sexual images;
- AI-generated sexual imagery;
- how to seek help without fear of being blamed.

The new model specifically includes:

- deepfakes and how to identify them;
- online misogyny;
- online content promoting violence or weapons;
- distorted/normalised harmful behaviours;
- escalation of conflict through social media;
- stalking;
- coercive and controlling behaviour;
- pornography and distorted representations of sex/relationships;
- commercial use of personal data;
- scams;
- sextortion;
- AI chatbots creating fake intimacy or offering harmful advice.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND.

In **Year 7 & 8,** students will be taught in their tutor PD Programme and IT lessons 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
- Life online – How can we make the internet safer?
- Why can't we always trust what we see in the media or online?
- How do we recognise the signs of online grooming?
- Social media – it is supposed to be fun, why is it also stressful?
- Cyber bullying and online trolls

In **Year 9,** students will have an internet safety unit as part of the tutor programme and in their PD lesson where they will learn:

- Financial exploitation and online scams (listed twice, likely taught in two sessions)
- Grief, loss and its digital legacy
- Why is my appearance online important

In **Year 10 and 11** students will be taught:

- Resilience, social media, trigger warnings and trauma
- Deepfakes: malicious use, the law and staying safe
- Body image, social media and eating disorders
- Social media and personal validation
- The dangers of cybercrime and the Dark Web
- 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
- Pornographic deepfakes and non-consensual image sharing
- Online dating
- Why are online privacy and data protection important?

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.

Practical Cybersecurity Skills

Students will be taught:

- methods hackers use to obtain personal information;
- password security;
- social engineering;
- physical security of devices;
- risks of USB/removable storage;
- multi-factor authentication;
- reporting cyber incidents/attacks;
- reporting personal data breaches.

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. Information will be shared about:

- the filtering and monitoring systems the school uses;
- what children are asked to do online;
- sites children will be asked to access;

- who from school they may interact with online;
- school expectations regarding appropriate pupil use of AI. 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 Headteacher.

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 Headteacher 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 Headteacher / 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 / Headteacher / 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

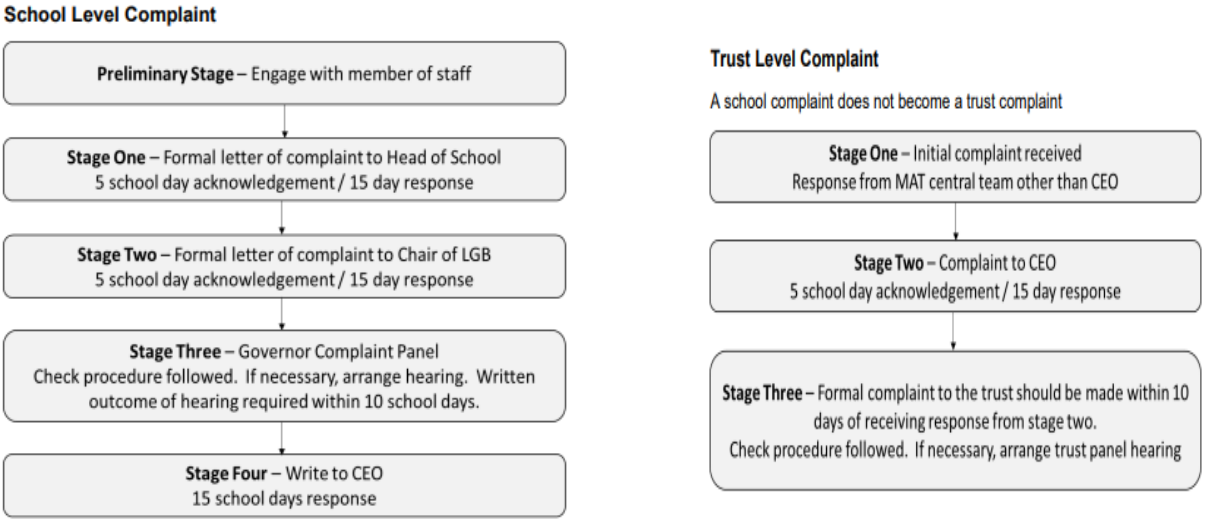
If a member of staff suspects that a device may contain an indecent image of a child, also known as a nude or semi-nude image, including any image that has been generated or altered using artificial intelligence (AI), they must not view, copy, print, share, store, save or forward the image. They must not ask a student to share or download the image.

- Staff must not delete the image or ask the student to delete it. They must not ask the student or students involved to disclose information about the imagery, as this is the responsibility of the DSL. Staff should not share information about the incident with other members of staff, students or parents/carers unless advised to do so by the DSL, and must not say or do anything that could blame or shame a student involved.
- The member of staff should confiscate the device and report the incident to the DSL immediately. The DSL will decide what action should be taken in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes.
- If a member of staff has already viewed the imagery accidentally, for example because a student showed it to them before they were able to intervene, they must report this to the DSL and seek appropriate support.

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



Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative AI tools and chatbots such as ChatGPT and Google Gemini.

HISP Trust and Thornden School recognise that AI has many potential benefits for teaching and learning, but that it can also create new safeguarding and online safety risks.

AI can be used to create false or manipulated images, audio and video that appear to be genuine. This includes 'deepfakes', 'deep nudes' and deepfake pornography, where AI is used to create or alter sexual or pornographic content using a person's likeness.

Thornden School will treat any use of AI to bully, harass, intimidate or cause harm to another student seriously and will respond in line with the school's Behaviour Policy and safeguarding procedures.

Staff must be aware of the potential risks associated with AI tools. Where new AI tools are introduced for use within the school, or where an existing AI tool is being used in a way which may pose a risk to students, staff or others, an appropriate risk assessment should be undertaken.

Any use of artificial intelligence by staff or students must be in accordance with the school's agreed expectations and any HISP Trust or Thornden School guidance relating to the use of AI.

Acceptable Use of IT Systems, Filtering and Monitoring

Students

All students are expected to follow the school's Acceptable Use Policy when accessing school IT systems, devices and the internet. IT systems must be used appropriately and for educational purposes.

Thornden School and HISP Trust use Smoothwall Cloud Filter across all managed school and Trust devices. Filtering remains active whether devices are being used in school or away from school, including when connected to home or other external networks.

Students should be aware that their use of school IT systems is subject to filtering and monitoring. Any inappropriate use of school IT systems that triggers a Smoothwall alert will be reviewed and followed up in line with the school's Behaviour and Safeguarding Policies. This may include discussions with students, contact with parents/carers, appropriate sanctions or safeguarding interventions, depending on the nature and seriousness of the concern.

Parents/carers are expected to support the school's acceptable use expectations and reinforce the importance of safe and responsible online behaviour.

Staff, Governors and Volunteers

All staff, governors and volunteers are expected to comply with the school's Acceptable Use Policy and relevant professional expectations when accessing school IT systems, devices and the internet. These systems should be used for educational purposes or to fulfil responsibilities associated with their role.

Thornden School and HISP Trust use Smoothwall Cloud Filter across all managed school and Trust devices. Filtering remains active both on and off site, including when devices are connected to external networks.

All adults should be aware that their use of school IT systems is subject to filtering and monitoring. Any Smoothwall alerts indicating potentially inappropriate use will be reviewed and, where necessary, followed up in accordance with the Staff Code of Conduct, relevant Trust policies and safeguarding procedures. Any subsequent action will be proportionate to the nature and seriousness of the concern.

Requests for Access to Curriculum-Related Websites

The school recognises that some curriculum areas, particularly Personal Development, Relationships and Sex Education (RSE) and safeguarding education, may require access to websites or online content that would ordinarily be restricted by the school's filtering arrangements.

Staff who require access to restricted websites or online resources for legitimate educational purposes should submit a request to the IT Team, outlining the website or resource required and its intended curriculum use.

The IT Team will liaise with the appropriate member of SLT to review the educational purpose of the request and consider any safeguarding implications before access is approved.

Staff must not attempt to bypass the school's filtering arrangements. Any approved changes will be managed by the IT Team, ensuring that appropriate safeguards remain in place.

Visitors

Visitors who are given access to the school's IT systems or internet are expected to read and comply with the school's acceptable use expectations where relevant.

Any inappropriate use of school IT systems or internet access by visitors will be reviewed and addressed in accordance with the school's safeguarding procedures and relevant Trust policies.

Filtering and Monitoring Arrangements

Thornden School and HISP Trust use filtering and monitoring systems to help protect students and adults from harmful, inappropriate or illegal online content and to support compliance with safeguarding and online safety requirements.

Smoothwall Cloud Filter operates across all managed school and Trust devices, regardless of whether they are connected to the school network or an external network. This provides a consistent level of online protection wherever a managed device is being used.

The school and Trust will regularly review filtering and monitoring arrangements to ensure that they remain effective, proportionate and appropriate to the safeguarding needs of students and the wider school community, without unreasonably restricting teaching and learning.

Filtering and monitoring alerts will be reviewed appropriately, recognising that an alert does not automatically indicate misconduct but may require further investigation or action depending on the circumstances. Any

concerns identified through monitoring will be addressed through the school's established behaviour, safeguarding or staff conduct procedures, as appropriate.

Students using mobile devices in school

Thornden School operates as a mobile phone-free environment during the school day.

Students may bring a mobile phone to school, but they are not permitted to access or use their mobile phone, or smart technology with similar functionality such as a smart watch, during the school day. This includes lessons, tutor time, movement between lessons, breaktime and lunchtime.

Students must comply with the school's agreed arrangements for securing or restricting access to mobile phones during the school day, including the use of the school's LOQT arrangements where applicable.

Any exception to these expectations will be agreed on an individual basis and must be authorised by the school. This may include arrangements to meet an identified medical, SEND or safeguarding need.

Where a student has an agreed exception, any use of a mobile device must still be in accordance with the school's Acceptable Use Policy and the specific arrangements agreed with the school.

Any breach of the school's mobile phone expectations may result in sanctions in accordance with the Behaviour Policy and may result in the device being confiscated.

Please see page 7-10 of Thornden School's Behaviour for Learning Policy for further information.

Staff using work devices outside school

Staff members using school or Trust-issued devices outside school must take all reasonable steps to ensure that the device and any information stored or accessed through it remain secure.

School and Trust-issued devices are provided for professional school and Trust business only and must be used in accordance with the Trust's ICT Acceptable Use Policy and all relevant safeguarding, information security and data protection requirements.

Staff must ensure that:

- devices are protected by a secure password or passphrase;
- passwords and passphrases are not shared with other people;
- devices are locked whenever they are left unattended;
- school or Trust devices are not shared with family members, friends or other unauthorised individuals;
- operating systems and security software are kept up to date;
- anti-virus and other security software provided by the school or Trust remains active;
- any school or Trust data stored or accessed through the device is appropriately protected;
- removable storage devices such as USB drives are encrypted where they contain school or personal data.

Filtering and safeguarding protections provided through **Smoothwall Cloud Filter** remain active on all managed school and Trust devices when they are used away from school, including when connected to home or other external internet networks.

Staff must not attempt to disable, bypass, interfere with or remove filtering, monitoring or security software installed on school or Trust devices.

Any concerns regarding the security of a device, including loss, theft, suspected compromise or concerns about the operation of filtering or monitoring software, must be reported to IT Support or the Trust Network Manager immediately.

This incorporates the additional device-security expectations in the updated model policy.

Staff using their own devices in school

Where staff use a personal device to access school systems or data, they must ensure that the device is secure and protected by an appropriate password or passphrase.

Staff must not use a personal device in any way that would breach the school's Acceptable Use Policy, Staff Code of Conduct, Data Protection Policy or safeguarding procedures.

Staff must take all reasonable steps to protect any school information accessed through a personal device. Devices must be locked when unattended and must not be shared with other individuals while school information is accessible.

Any suspected loss, theft, unauthorised access or data breach must be reported immediately in accordance with the school's data protection procedures and to IT Support.

Where required, personal devices which have been used to access school systems may need to have school-licensed software, accounts or school data removed when employment ends.

How the school will respond to issues of misuse

Where a student misuses the school's IT systems, internet or online services, the school will respond in accordance with the Behaviour Policy and Acceptable Use Policy. The action taken will depend upon the individual circumstances and the nature and seriousness of the incident and will be proportionate.

Where a member of staff misuses the school's IT systems or internet, or uses a personal device in a way that constitutes misconduct, the matter will be dealt with in accordance with the Staff Code of Conduct and relevant disciplinary procedures.

The school will consider whether any incident involving illegal activity, illegal content or other serious concerns should be reported to the police or another appropriate external agency.

Training

All new staff will receive training as part of their induction on safe internet use and online safeguarding issues, including cyber-bullying, online abuse and the risks of online radicalisation.

All staff will receive refresher training at least once each academic year as part of safeguarding training, together with relevant updates during the year as required.

Through this training, staff will be made aware that technology is a significant component of many safeguarding and wellbeing issues and that children may experience abuse online.

Children may abuse their peers online through, for example:

- abusive, threatening, harassing or misogynistic messages;
- the non-consensual sharing of nude or semi-nude images or videos, including images that have been generated or altered using AI;
- the sharing of abusive images or pornography, including content generated or altered using AI, with individuals who do not wish to receive it.

Staff will also understand that physical abuse, sexual violence, sexual harassment and initiation or hazing-type behaviours may contain an online element.

Training will support staff to recognise signs of online harm, understand emerging risks and help students recognise dangers, assess risks and make safer choices online.

The DSL and Deputy DSLs will undertake appropriate safeguarding training which includes online safety and will update their knowledge and skills regularly and at least annually.

Monitoring arrangements

The DSL will ensure that safeguarding concerns relating to online safety are appropriately recorded on CPOMS and managed in accordance with the school's safeguarding procedures.

Behaviour incidents relating to online safety will also be recorded and managed through the school's appropriate behaviour and recording systems.

The effectiveness of the school's filtering and monitoring arrangements will be reviewed at least annually, with appropriate involvement from the DSL, senior leaders, IT staff and governors.

This policy will be reviewed annually. The review will be supported by an annual assessment of the online risks faced by students, recognising that technology and the associated risks and harms continue to develop rapidly.

At each review, the policy will be presented to the Academy Committee for approval.

Links with other policies

This policy should be read alongside the school's:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Code of Conduct and disciplinary procedures
- Data Protection Policy and privacy notices
- Complaints Procedure
- Mobile Phone Policy and/or school mobile phone arrangements
- Artificial Intelligence guidance or policy, where applicable
- Searching, Screening and Confiscation procedures

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: ……