Online Safety Policy

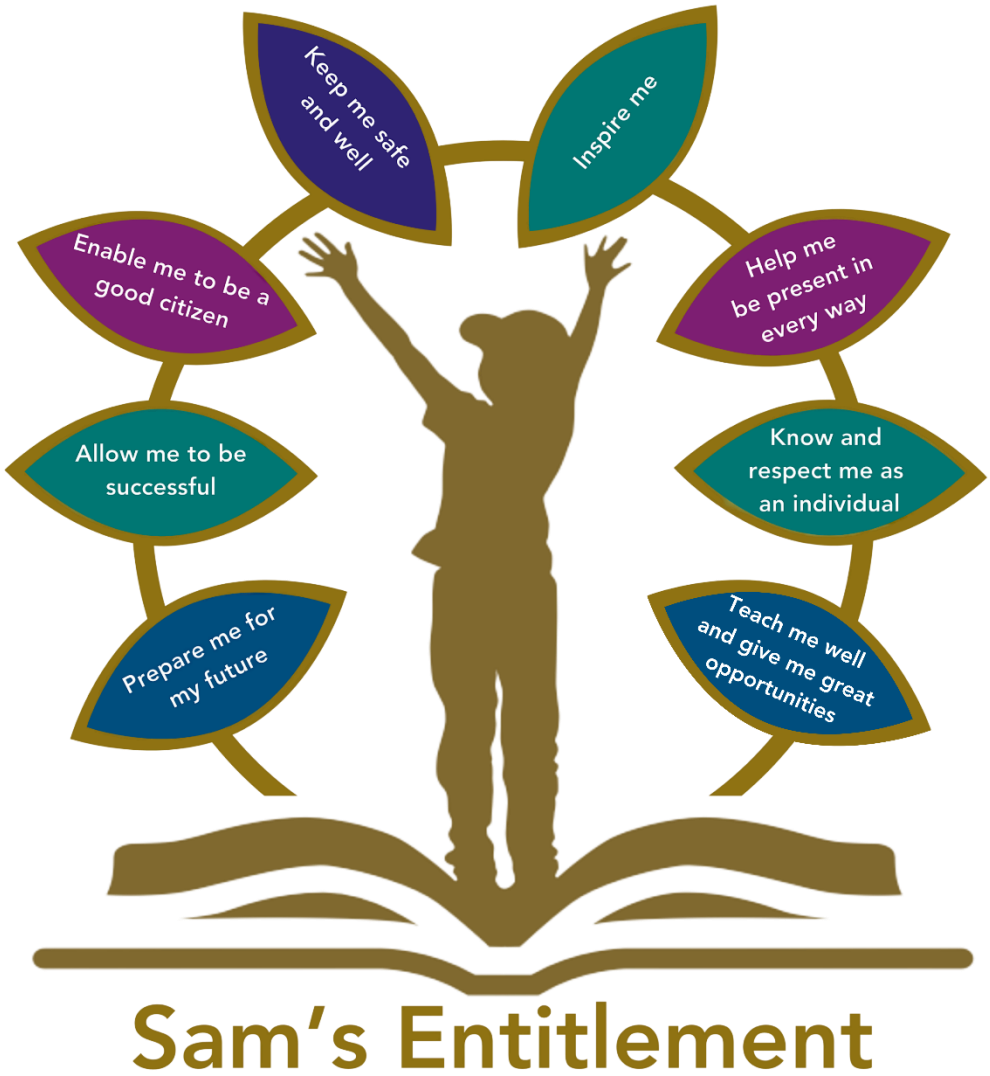
Reviewed on	Sept 2026	Review frequency	Annually
Next review due	Aug 2027	Template Yes / No	No
Owner	Director of IT	Approved by	Executive

1. History of Policy Changes

Date	Page	Change	Origin of Change
12/08/2026	5	Added MS team in the responsibilities section	
12/08/2026	8	Filtering & Monitoring: New section added	

2. Contents

1. History of Policy Changes 2
2. Contents 2
3. Introduction 3
4. Scope 4
5. Roles and Responsibilities 5
6. Use of Digital Technologies 7
7. Filtering and Monitoring 8
8. Add Online Reputation and Digital Footprint 8
9. Educating Pupils about Online Safety 9
10. Educating Parents about Online Safety 11
11. Cyber-bullying 11
12. Artificial intelligence (AI) 12
13. Acceptable Use of IT at HET/School 13
14. Reporting Abuse 14
15. Training 15
16. Link to other HET policies 15



3. Introduction

Hamwic Education Trust (HET) believe that all pupils should receive a high quality, enriching, learning experience in a safe and inclusive environment, which promotes excellence through a broad curriculum that prepares them for their future and opens doors to a diverse array of opportunities as well as that all pupils and adults within HET flourish as individuals and together.

This Online Safety Policy outlines the commitment of Hamwic Education Trust (HET) and its schools to safeguard members of our school community online in accordance with statutory guidance and best practice.

HET will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

As part of our commitment to learning and achievement we at HET and its schools, want to ensure that the internet and other digital technologies are used to:

- Raise educational standards and promote pupil achievement

- Develop the curriculum and make learning exciting and purposeful
- Enable pupils to gain access to a wide span of knowledge in a way that ensures their safety and security

To enable this to happen we have taken a whole HET/School approach to online safety as promoted by Online Safety Act 2023, which includes the development of policies and practices, the education and training of employees and pupils and the effective use of the HET/School's IT infrastructure and technologies.

HET, as part of this policy, holds steadfastly to the ethos that there should be an equitable learning experience for all pupils using ICT technology. We recognise that ICT can allow disabled pupils increased access to the curriculum and other aspects related to learning.

HET is committed to ensuring that all its pupils will be able to use existing, as well as up and coming technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents, are educated as to the dangers that exist so that they can take an active part in safeguarding them.

Our approach to online safety is based on addressing the following categories of risk as set out by the Keeping children safe in education (KCSIE) statutory guidelines:

- **Content**: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **Contact**: being subjected to harmful online interaction with other users; for example: 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**: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.
- **Commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

HET recognises that online safety cannot be achieved through technology alone. Effective online safety requires a combination of education, appropriate filtering and monitoring, clear policies, cyber security controls, staff vigilance and strong safeguarding processes.

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for HET/School on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- It also refers to the DfE's guidance on protecting children from radicalisation.

4. Scope

This Online Safety Policy applies to all members of the HET community (including employees, pupils, volunteers, parents and carers, visitors, community users) who have access to and are users of HET/School digital systems, both in and out of HET/School. It also applies to the use of personal digital technology on HET/School site (where allowed).

5. Roles and Responsibilities

Local/Trust Governors:

The HET Board and local governance committee has overall responsibility for monitoring this policy and holding the HET/School SLT to account for its implementation. It will

- Ensure all employees undergo online safety training as part of child protection and safeguarding training, and ensure employees understand their expectations, roles and responsibilities around filtering and monitoring.
- The Trustees/Governors will co-ordinate regular meetings with appropriate employees to discuss online safety and requirements for training and monitor online safety logs as provided by the designated safeguarding lead (DSL).
- The Trustees/Governors will make sure that HET/School teaches pupils how to keep themselves and others safe, including online.
- Will make sure that HET/School has appropriate filtering and monitoring systems in place

Managed Services Team

The Managed Services Team is responsible for:

- Creating and maintaining this policy in line with the latest legislation.
- Ensuring cyber security controls are maintained.
- Providing online safety advice and guidance to schools.
- Supporting incident investigation and evidence gathering.
- Maintaining oversight of trust-wide online safety trends and risks.

School Leaders

- The school leader is responsible for ensuring that employees understand this policy, and that it is being implemented consistently throughout the school
- The school leaders are responsible for ensuring that the DSL/DDSL and other relevant employees receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant
- The school leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role
- The senior leadership team will receive regular monitoring reports from the DSL/DDSL

Designated Safeguarding Lead

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

- Supporting the school leader in ensuring that employees understand this policy and that it is being implemented consistently throughout the school
- Working with the school leader, HET IT team and other employees, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Updating and delivering employee training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governance team
- Providing regular safeguarding and child protection updates, including online safety, to all employees, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

- Ensure that all employees are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Liaises with HET for any guidance, updates and reporting
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments

This list is not intended to be exhaustive.

Technical Employees

The technical employees (HET IT team) is responsible for ensuring:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on HET/School devices and HET/School networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at HET/School, including terrorist and extremist material.
- Making sure that the HET/School's IT systems are secure, is not open to misuse or malicious attack, and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the HET/School's IT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- That users must access systems through secure authentication methods including strong passwords and multifactor authentication where available.
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- That monitoring software and systems are implemented and updated as agreed in HET/School policies.

This list is not intended to be exhaustive

Teaching and Support Employees

are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current HET/School online safety policy and practices.
- They have read, understood and signed the employees acceptable use policy (AUP).
- They report any suspected misuse or problem to the senior leader/DSL.
- All digital communications with pupils/parents/carers should be on a professional level and only carried out using official HET/School systems.
- Online safety issues are embedded in all aspects of the curriculum and other activities .
- They monitor the use of digital technologies, mobile devices, cameras etc. In lessons and other HET/School activities (where allowed) and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Training has been provided to them around online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:
    - sharing of personal data
    - access to illegal/inappropriate materials
    - inappropriate on-line contact with adults/strangers
    - potential or actual incidents of grooming

- cyber-bullying
- use of HET/School devices outside of the HET/School network (Laptops/Tablets taken home for work), should be used in safe environments, and any sensitive data kept secure.

Pupils

- are responsible for using the HET/School digital technology systems in accordance with the pupil acceptable use policy.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school.

Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. HET/School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local online safety campaigns.

Parents and carers will be encouraged to support HET/School in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at HET/School events
- access to parents' sections of the website and online pupil records
- their children's personal devices in HET/School (where this is allowed)

Community Users

Community users who access HET/School systems/website as part of the wider HET/School provision will be expected to sign a community user Acceptable Use Policy before being provided with access to HET/School systems.

6. Use of Digital Technologies

HET will seek to ensure that internet, mobile and digital technologies are used effectively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk.

HET expects all employees and pupils to use the internet, mobile and digital technologies responsibly and strictly according to the conditions below. These expectations are also applicable to any voluntary, statutory and community organisations that makes use of the HET's IT facilities and digital technologies.

Users shall not visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children
- Promoting discrimination of any kind
- Promoting racial or religious hatred
- Promoting illegal acts

- Any other information which may be offensive to peers or colleagues.

HET recognises that in certain planned curricular activities, access to otherwise deemed inappropriate sites may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned and recorded so that it can be justified if required.

Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the material that is deemed inappropriate or of huge concern may be reported to the police and will also be subject to internal sanctions in accordance with behaviour policies and/or employees conduct.

Emerging Technologies

HET recognises that technology develops rapidly and that new digital services may introduce new safeguarding risks.

HET/Schools will regularly review emerging technologies, including artificial intelligence, immersive technologies, social media platforms, messaging services and online gaming environments, and update education, filtering, monitoring and safeguarding arrangements where required.

7. Filtering and Monitoring

HET filtering and monitoring support provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and technical staff to be effective. The DSL will have lead responsibility for safeguarding, online safety and the filtering and monitoring support provider will have technical responsibility.

- The filtering & monitoring provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering and monitoring
- HET manages access to content across its systems for all users and on all devices using the HET/School's internet provision
- HET monitors all network use across all its student devices and services.
- Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.
- Devices that are provided by HET/School have HET/School based filtering & monitoring applied irrespective of their location.
- Where all students have logins, filtering & monitoring enables alerts to be matched to users and devices.
- Filtering and monitoring alerts are reviewed by authorised safeguarding and/or technical personnel in accordance with agreed processes and risk thresholds. Where safeguarding concerns are identified, appropriate action will be taken and recorded.

8. Add Online Reputation and Digital Footprint

Pupils will be educated about the importance of maintaining a positive online reputation and understanding that online actions can create a long-lasting digital footprint.

Pupils should understand that information, images and comments shared online may remain accessible even after deletion.

9. Educating Pupils about Online Safety

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

Key Stage 1

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Key Stage 2

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
- Be discerning in evaluating digital content

By the end of primary school, pupils will know:

- That the internet can be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health
- 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, 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 are shared and used online
- How to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- Why social media, computer games and online gaming have age restrictions and how to manage common difficulties encountered online
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- Where and how to report concerns and get support with issues online
- How anything that is posted or put online creates a digital footprint of themselves that can be searchable by anyone

Key Stage 3

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

Key Stage 4

Pupils in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the end of secondary school, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- The characteristics of social media, including that some social media accounts are fake, and/or may post things which aren't real/have been created with AI. That social media users may say things in more extreme ways than they might in face-to-face situations, and that some users present highly exaggerated or idealised profiles of themselves 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. Pupils should understand that any material provided online might be circulated, and that once this has happened there is no way of controlling where it ends up. Pupils should understand the serious risks of sending material to others, including the law concerning the sharing of images
- What to do and how to report when they are concerned about material that has been circulated, including personal information, images or videos, and how to manage issues online
- About the prevalence of deepfakes including videos and photos, how deepfakes can be used maliciously as well as for entertainment, the harms that can be caused by deepfakes and how to identify them
- That the internet contains inappropriate and upsetting content, some of which is illegal, including unacceptable content that encourages misogyny, violence or use of weapons. Pupils should be taught where to go for advice and support about something they have seen online. Pupils should understand that online content can present a distorted picture of the world and normalise or glamorise behaviours which are unhealthy and wrong
- That social media can lead to escalations in conflicts, how to avoid these escalations and where to go for help and advice
- How to identify when technology and social media is used as part of bullying, harassment, stalking, coercive and controlling behaviour, and other forms of abusive and/or illegal behaviour and how to seek support about concerns
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)
- How information and data is generated, collected, shared and used online
- That websites may share personal data about their users, and information collected on their internet use, for commercial purposes (e.g. to enable targeted advertising)

- That criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion
- That AI chatbots are an example of how AI is rapidly developing, and that these can pose risks by creating fake intimacy or offering harmful advice. It is important to be able to critically think about new types of technology as they appear online and how they might pose a risk

10.Educating Parents about Online Safety

HET schools 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.
Online safety will also be covered during parents' evenings/mornings/assemblies, etc.

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

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

Concerns or queries about this policy can be raised with any member of employees or the headteacher.

11.Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power.

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. Teachers will discuss cyber-bullying with their tutor groups.

Teaching employees 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.

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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining Electronic Devices

The headteacher, and any employees authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to employees 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, the authorised employees will:

- Assess how urgent the search is, and consider the risk to other pupils and employees
- 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 cooperation

Authorised employees 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 employees should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of HET/School or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to HET/School to decide on a suitable response. If there are images, data or files on the device that employees 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, employees 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, employees 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 refuses to delete the material themselves

If an employee **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 complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through HET/School complaints procedure

12.Artificial intelligence (AI)

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

HET 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. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

HET will treat any use of AI to bully pupils very seriously, in line with our behaviour policy.

Pupils using AI technologies must be taught how to use them safely, ethically and critically. Pupils should understand that AI-generated content may be inaccurate, misleading, biased or entirely fabricated and must not automatically be considered factual.

Employees should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the HET/School, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and employees.

All employees should have read and understood the HET AI guidance and ensure that they adhere to the use of AI in accordance with this guidance.

Personal, safeguarding, confidential or assessment information must not be entered into AI services unless the service and use have been approved by HET.

13.Acceptable Use of IT at HET/School

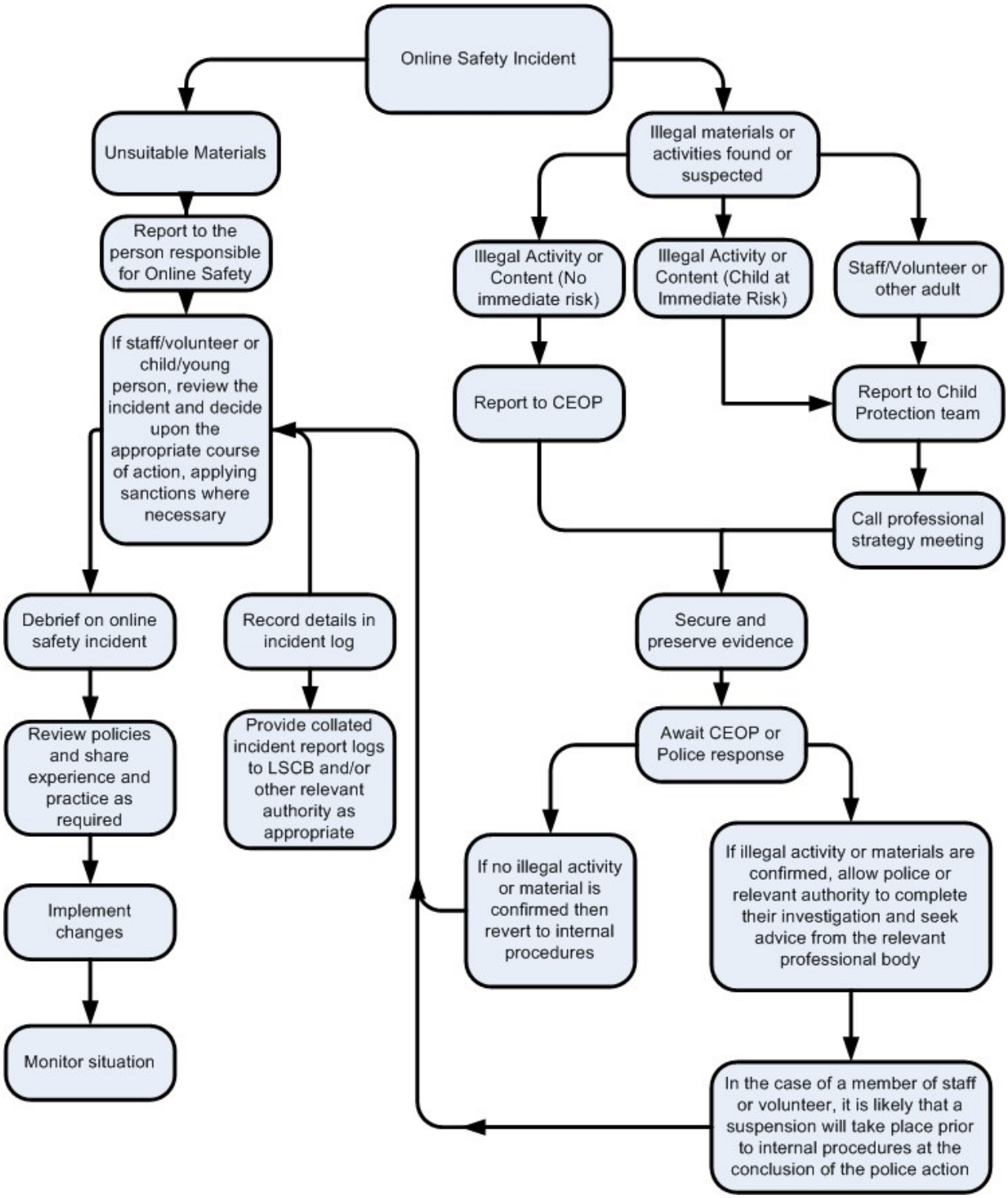
All pupils, parents, employees, volunteers and governors are expected to sign an agreement regarding the acceptable use of the HET/School's IT systems and the internet. Visitors will be expected to read and agree to the HET/School's terms on acceptable use if relevant.

Use of the HET/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, employees, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

14.Reporting Abuse

The following outlines what to do if a child or adult receives an abusive email or accidentally accesses a website that contains abusive material.



CEOP – Child Exploitation and Online Protection
LSCB – Local Safeguarding Children Board

15.Training

All new employees 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 employees 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 employee's meetings).

By way of this training, all employees 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 employees:

- 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

16.Link to other HET policies

- Acceptable use policy
- AI Guidance
- Behaviour policy
- Complaints procedure
- Child protection and safeguarding policy
- Data protection policy and privacy notices
- Employees Handbook