Online Safety Policy

Reviewed on	Aug 2025	Review frequency	Annually
Next review due	Sept 2026	Template Yes / No	No
Owner	J Solanki	Approved by	Executive

1. History of Policy Changes

Date	Page	Change	Origin of Change

2. Contents

1. History of Policy Changes 2
2. Contents 2
3. Introduction 3
4. Scope 4
5. Definitions 4
6. Roles and Responsibilities 5
7. Use of Digital Technologies 7
8. Educating Pupils about Online Safety 8
9. Educating Parents about Online Safety 9
10. Cyber-bullying 9
11. Artificial intelligence (AI) 10
12. Acceptable Use of IT in school 11
13. Reporting Abuse 12
14. Training 13
15. Link to other HET policies Acceptable use policy 13



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.

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

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 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 school's ICT 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:

- **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
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

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
- It also refers to the DfE's guidance on protecting children from radicalisation.

4. Scope

This policy is for all employees working within a HET school or establishment (which for ease of reference are referred to throughout this document as 'schools') or the HET Managed Service (MS) Team.

5. Definitions

- 'Local Governing Committee' in this policy, where reference is made to the Governing Committee, this means the Local Governing Committee of the school, or the Trust in the case of a school where no Local Governing Committee is present. Where a Governing Committee is not present in a school, or numbers are low, Governors from other schools/partnerships may be used.
- 'Manager' in this policy, is anyone as identified in the staffing structure with line management responsibilities.

6. Roles and Responsibilities

Local/Trust Governors:

The Trust Board and local governance committee has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. It will

- make sure 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 governance team 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 governance team will make sure that the school teaches pupils how to keep themselves and others safe, including online.
- will make sure that the school has appropriate filtering and monitoring systems in place

School Leaders

- The school leader is responsible for making sure 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(s)

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

- Supporting the headteacher in ensuring that employees understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager 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

(NOTE: If the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school technical employees, as suggested below. It is also important that the managed service provider is fully aware of the school's online safety policy and procedures.)

The technical employees is responsible for ensuring:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and 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 school, including terrorist and extremist material
- Making sure that the school's ICT 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 school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- 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 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 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 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 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 school devices outside of the 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 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. The 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 the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

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

Community Users

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

7. 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 school's ICT 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.

8. 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

9. Educating Parents about Online Safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. 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.

10. 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:

- Make an assessment of 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 the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the Trust/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 a employees **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 the school complaints procedure

11. 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.

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 school/trust, 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 to this guidance.

12. Acceptable Use of IT in school

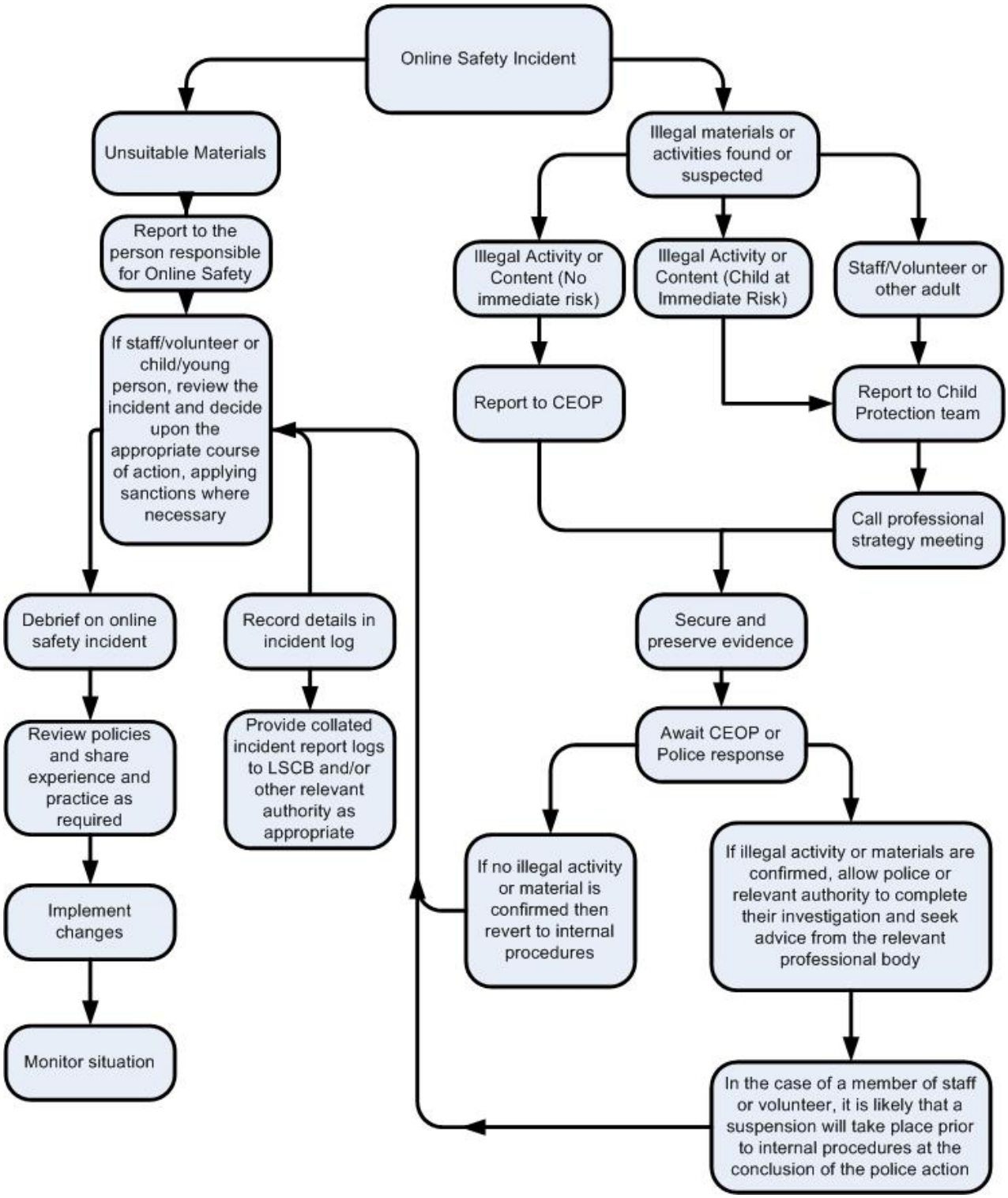
All pupils, parents, employees, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, employees, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

13. 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

14. 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 employees 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

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.

The governance team 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.

15. 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