To inspire, enrich and nurture so each individual reaches their full potential

Hatfield Community Free School, Briars Lane, Hatfield, Herts, AL10 8ES
Website: www.hcfs.org.uk **Telephone:** 01707 276018 **Email:** office@hcfs.org.uk

@hatfieldcfs1 @hatfieldcfs

Principal: Mrs Victoria Hobson

The HCFS is a company limited by Guarantee Registration number 07648654

Online Safety Policy

September 2025

To be reviewed annually in the Autumn Term

Next Review: September 2026

History of Document:

Issue No.	Date Issued	Prepared By	Approved By	Comments
Issue 1	September 2017	Jane Sutton	Martine Archer	Policy Created
Issue 2	September 2021	Jane Sutton	Victoria Hobson	Name changes
Issue 3	September 2022	Martha Surry	Victoria Hobson	• Additional sections added to reflect KCSIE 2022 • Removal of reference to IT Specialists
Issue 4	September 2023	Victoria Hobson	Victoria Hobson	Updated in line with KCSIE 2023 and model policies on The Grid and The Key
Issue 5	September 2024	Martha Surry	Victoria Hobson	• Updated in line with KCSIE 2024 • Names and job titles updated in section 3
Issue 6	September 2025	Martha Surry	Victoria Hobson	• Edits/updates in section 3, 6.3, 6.3.1, 6.4, 6.5, 7, 9.2, 9.4, 13, 14, Appendix One and Two • New section – 13.1

Table of Contents

1. Introduction

At Hatfield Community Free School (HCFS), we take our responsibilities for online safety very seriously through having high expectations of learning, behaviour and respect for each other underpinning everything we do. Our teachers strive to create independent, articulate thinkers and learners who have the confidence to achieve their ambitions. This drives us in our pursuit for excellence every day in a kind a respectful way. Our core values are at the heart of what we value and support.

HCFS recognises that internet, mobile and digital technologies provide positive opportunities for children and young people to learn, socialise and play but they also need to understand the challenges and risks. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that all pupils, staff and trustees will be supported to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in helping children and young people navigate the online world safely and confidently.

2. Philosophy

At HCFS the development of all children's social, moral, spiritual and cultural growth is paramount. We believe that the most important function of the school is to maintain an environment in which every member of the school is able to achieve success and self-fulfilment. There must be a total consistency of expectation that everyone (irrespective of gender, race or culture) should feel safe and secure, have empathy for all others, and place a high value upon individual achievement and personal development.

3. Safeguarding Children

HCFS is committed to safeguarding and promoting the welfare of children. Applicants must be willing to undergo child protection screening appropriate to the post, including with past employers and the Disclosure and Barring Service (DBS). If we have any concerns with regards to safeguarding relating to our children, we have a duty of care to report it to the Designated Safeguarding Person, Mrs Victoria Hobson (Principal), Miss Joanne Pape (Vice Principal), Mrs Ellen Summers (Assistant Vice Principal Pastoral) or Mrs Ashley Holmes (SENDCO). Our safeguarding trustee is Sarah Adler and our Chair of Trustees is Maxine Kinghorn. For further information, please refer to our Child Protection Policy.

4. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and trustees;
- Identify and support groups of pupils that are potentially at greater risk of harm online than others;
- 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 (which we refer to as 'mobile phones');
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

4.1 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, misinformation, disinformation (including fake news), conspiracy theories, 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 the user for sexual, criminal, financial or other purposes
Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

5. Writing, agreement and review of the Online safety policy

Our Online safety policy has been written by the school using Hertfordshire Local Authority and Government advice. It has been agreed by the Senior Leadership Team. This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

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

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

The policy and its implementation will be reviewed annually.

6. Roles and Responsibilities

6.1 The Trust Board

The Trust Board has overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

The Trust Board will make sure all staff undergo online safety training as part of child protection training and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring. In addition, they will also ensure all staff receive regular online safety updates as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

They will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding leads (DSL).

The Trust Board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The Trust Board 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 board will review the DfE filtering and monitoring standards, and discuss with the Senior Leadership Team 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 trustees will:

- Ensure that they have read and understand this policy;
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet;
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures;
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

6.2 The Principal

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

6.3 The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our Child Protection Policy, as well as relevant job descriptions.

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

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school;
- Working with the Principal and trust board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly;
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks;
- Working with the ICT team to make sure the appropriate systems and processes are in place;
- Working with the Principal, ICT team and other staff, as necessary, to address any online safety issues or incidents;
- Managing all online safety issues and incidents in line with the school's child protection policy;
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy;
- Updating and delivering staff training on online safety; (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary;
- Providing regular reports on online safety in school to the Principal and/or Trust Board;
- Undertaking annual risk assessments that consider and reflect the risks pupils face;
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

This list is not intended to be exhaustive.

6.3.1 Filtering Internet Content

In a perfect world, filtering would be 100% accurate and inappropriate material would not be visible to pupils using the Internet. In practice this is not easy to achieve and cannot be guaranteed. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable and threatening. Such a procedure will be detailed further into this policy.

The school will ensure:

- Systems are in place to filter website content;
- Classroom staff will make checks to ensure that the filtering is appropriate, effective and reasonable and this is monitored regularly;
- A local school list (blocked) will be maintained to further control the websites available within the school.

If for any reason, the filtering blocks a website that a class teacher feels would be of benefit to the children then it can be added to a limited usage category and therefore be unblocked for teacher/pupil use. Such additions should be made to the Principal who will make a decision on whether or not to add the website to the limited list.

Further information about internet filtering can be found in our Filtering and Monitoring Policy.

6.4 The ICT Team

The ICT team, as directed by the DSL team, is responsible for:

- 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 ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material;
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly;
- Conducting a full security check and monitoring the school's ICT systems on a termly basis;
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;
- Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy;
- Making sure 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.

6.5 All staff and volunteers

All staff, including contractors and agency, and pupils will be expected to take responsibility for their use of the network. As part of their daily use they can be reasonably expected to:

- Maintain an understanding of this policy;
- Implement this policy consistently;
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use;
- Knowing that the DSP 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;
- Following the correct procedures by liasing with a member of the DSP team if they need to bypass the filtering and monitoring systems for educational purposes;
- 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;
- 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';
- Keep their password secret from peers;

- Ensure that they securely logoff from any workstation they use during the day;
- Act to ensure they speed of the network by selecting the most appropriate time to download large resources or watch on-line TV content;
- Clean up unused files from the network to assist with the longevity of disk storage devices;
- Ensure the removal of any portable storage devices or media;
- Password protect any confidential or sensitive information;
- Not open any attachments, executables or files from unknown or untrusted sources;
- Report any concerns or possible breaches of security to the Principal;
- Realise that school ICT space is not personal space;
- Not take copies of any materials that belong to or are the intellectual property of the school;
- To leave copies of any planning or resources, created using IT, that are required by the school.

6.6 Parents and Carers

Parents and carers are expected to:

- Notify a member of staff or the SLT of any concerns or queries regarding this policy;
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

6.7 Visitors

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

7. Educating pupils about online safety

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

All schools have to teach: Relationships education and health education in primary schools.

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.

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.

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

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

8. Educating parents/carers about online safety

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

The school will let parents/carers 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/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the DSL Team or Principal.

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

9. Cyberbullying

9.1 Definition

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

9.2 Preventing and addressing cyber-bullying

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

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

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

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will 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.

9.3 Examining electronic devices

The Principal and any member of staff authorised to do so by the Principal (as set out in your behaviour policy) 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 Principal;
- 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.

Authorised staff members 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 senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person; and/or
- The pupil and/or the parent/carer refuses to delete the material themselves.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image;
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation;
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people;
- Our behaviour policy.

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

9.4 Artificial intelligence (AI)

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

HCFS 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.

HCFS will treat any use of AI to bully pupils in line with our anti-bullying policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the 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 staff.

10. Acceptable usage

All pupils, parents/carers, staff, volunteers and trustees 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, staff, volunteers, trustees and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

10.1 E-Mail

Directed e-mail use can bring significant educational benefits, however the use of e-mail requires that appropriate safety measures are also put into place. At HCFS, incoming and outgoing e-mail is limited within the school network for pupils but staff will have external access.

All school provided e-mail accounts are filtered and subject to monitoring in the following ways:

- Pupils may only use approved e-mail accounts on the school system;
- Pupil access to external e-mail addresses is not permitted;
- Staff will be encouraged not to access external e-mail accounts at school. Any access during directed teaching time is strictly forbidden;
- Pupils must immediately tell a teacher if they receive an offensive e-mail;
- Pupils must not reveal details of themselves or others, such as their address or telephone number, or arrange to meet anyone through e-mail communication;
- The forwarding of chain letters is banned;
- Official e-mail sent to parents should be written carefully and authorised before sending;
- Staff should ensure all emails sent to professional organisations are professional and courteous;

10.2 The management and publication of content

In this age, the use of websites to showcase a school and the work it produces has become extremely popular. However, it does provide opportunities acquiring sensitive and personal data if consideration is not given to the material available. The publication of pupil faces and full names is not acceptable. These published images could be re-used especially if a large image has been used. In addition to this, the publication of names and contact details of staff is discouraged and where necessary, access to this information will be available via other methods or through a secure portal.

- Only the schools contact details will be published. Staff or pupil contact information will not be published. The senior leadership team will take editorial responsibility and ensure content is accurate and appropriate. At all times, intellectual property and copyright rights will be respected and complied with.
- Under no circumstances is a pupils' full name to be published anywhere on a website when it might relate to a photograph;
- Parents will be given the right to 'opt out' of digital publication in any form of their child on the internet;
- The 'opt out' information will be updated annually and records will be kept;
- At all times, the pupils in photographs should, of course, be appropriately clothed.

10.3 Social Networking and personal publishing

The recent upsurge in the popularity of social networking sites such as Facebook, Snapchat, Instagram and Twitter requires schools to be aware of the potential dangers to staff and pupils. It has become much easier for individuals to publish content and information about themselves on the Internet. The risk of identity theft and the misuse of published photographic material should be considered as risks by all and appropriate steps to educate and protect staff and pupils be made.

- All social networking sites will be blocked in school for pupils;
- Consideration will be given, at all times, on how to educate pupils in their safe use;
- Pupils will be advised never to give out information that will identify themselves, their friends or their location;
- Pupils will be directed towards moderated sites;
- Pupils will be advised to use nicknames and avatars when using social networking sites;
- Pupils will be encouraged not to publish photographic content of themselves;
- Staff should not identify pupils of their place of work in status updates;
- Staff will be advised not to accept requests from current or past pupils or parents;
- Staff must not publish photographic content that contains any images from school or of pupils or parents;
- Staff should not publish status updates regarding school life.

10.4 Video Conferencing and webcams

The rapid expansion of communications technology requires the school to have a policy on its potential use in education.

- All video conferences and webcams must make use of the school network to ensure quality of service and security;
- Teachers must request permission from senior leadership team before making a call or using a webcam in a lesson;
- All webcam use will be supervised;
- At no point will any live streaming from school be permitted to be viewed on the Internet or through the school website.

10.5 Managing new technologies

Small wireless devices provide more opportunities for pupils to be exposed to content within school that cannot be controlled or filtered through the school network or security systems.

This can even extend to games consoles used in after school care clubs where it is possible to connect to global gaming networks and interact with other people. At all times, we need to be aware of the current technology and its possible risk and educational benefit.

Pupils' mobile phones will be permitted in school for safety reasons from Year 5 onwards only but they should be switched off during school hours and be stored in the designated space near the office and not be used within the school grounds.

Wearable technology, such as smart watches are not permitted to be connected to internet during the school day.

11. Staff using technology outside of school

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

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol);
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device;
- Making sure the device locks if left inactive for a period of time;
- Not sharing the device among family or friends;
- Installing anti-virus and anti-spyware software;
- Keeping operating systems up to date by always installing the latest updates.

Staff members must not use the device in any way which would violate the school's terms of acceptable use. Work devices must be used solely for work activities.

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

12. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

13. Training

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

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse;
- Children can abuse their peers online through:
  - Abusive, harassing and misogynistic messages;
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups;
  - Sharing of abusive images and pornography, to those who don't want to receive such content;
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse;
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks;
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL and deputies 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.

Trustees will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

13.1 Training pupils

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information;
- Password security;
- Social engineering;
- The risks of removable storage devices (e.g. USBs);
- Multi-factor authentication;
- How to report a cyber incident or attack;
- How to report a personal data breach.

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

14. Monitoring Arrangements

This policy will be reviewed every year by a member of the senior leadership team. At every review, the policy will be shared with the Trust Board. The review (such as the one available here) will be supported by an annual

risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Appendix One: Staff, Trustees, Contractors and Visitors Conduct rules

Please tick ✓

- I will ensure that I keep my password safe;
- I will ensure that I securely logoff from any workstation I use during the day;
- I will safeguard the speed of the network by selecting the most appropriate time to download large resources or watch on-line TV content;
- I will clean up unused files from the network to assist with the longevity of disk storage devices;
- I will ensure I remove any portable storage devices or media that I use in the school computers;
- I will password protect any confidential or sensitive information that I store on portable storage devices;
- I will not open any attachments, executables or files from unknown or untrusted sources;
- I realise that school ICT space is not personal space;
- I will not take copies of any materials that belong to or are the intellectual property of the school;
- I will leave copies of any planning or resources, created using IT, that are required by the school;
- I will not use the school IT equipment for personal financial gain, gambling, political activity, advertising or illegal purposes;
- I will not to reveal personal information about the pupils I teach or the school through email, personal publishing, blogs or messaging;
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance;
- I will not install any software or hardware without permission;
- I will not access or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely;
- I will report any incidents of concern regarding children's safety to the Designated Safeguarding Lead or SLT;
- I will promote online safety with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing especially on social media sites.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

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

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

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

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.
I have read and understand the rules of IT use.

Signed Date:

Appendix Two: Pupils IT Rules in Class or Groups

These rules help us to stay safe on the Internet:

1. We ask permission before using the Internet;
2. We only use websites that an adult has chosen;
3. We tell an adult if we see anything we are uncomfortable with; select a website by mistake, receive messages from people we don't know
4. I will tell a teacher if I find anything that may upset or harm me or my friends
5. We immediately close any webpage we not sure about;
6. We send e-mails that are polite and friendly;
7. We never give out personal information or passwords;
8. We never arrange to meet anyone we don't know;
9. We do not open e-mails sent by anyone we don't know;
10. We do not use Internet chat rooms;
11. We do not use You Tube or other video websites in school;
12. Always use the school's ICT systems and the internet responsibly and for educational purposes only;
13. We only use log in and details and usernames that are assigned to us.

We the undersigned agree to these rules.

Signed Date:

Appendix Three: Online Safety Training Needs Audit

Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, trustees and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	