Great Learners Trust

Inspiring Excellence | Empowering Futures

ELMHURST SCHOOL

ASPIRE. CREATE. THINK.

# Online Safety Policy

| | |
|---|---|
| **Approved by:** | Trust Board |
| **Approval period:** | Autumn Term 2026 – Autumn Term 2027 |
| **Review cycle:** | Annual |
| **Policy Source:** | The Key Model Policy |

# Contents

1. Aims ..... 3
2. Legislation and guidance ..... 3
3. Roles and responsibilities ..... 4
4. Educating pupils about online safety ..... 7
5. Educating parents/carers about online safety ..... 8
6. Cyber-bullying ..... 8
7. Acceptable use of the internet in school ..... 10
8. Pupils using mobile devices in school ..... 10
9. Staff using work devices outside school ..... 11
10. How the school will respond to issues of misuse ..... 11
11. Training ..... 12
12. Monitoring arrangements ..... 12
13. Links with other policies ..... 13

Appendix 1: Acceptable use of the internet: agreement for parents and carers
Appendix 2: KS2 Acceptable use agreement
Appendix 3: EYFS and KS1 acceptable use agreement
Appendix 4: Acceptable use agreement for staff, governors, volunteers and visitors
Appendix 5: online safety training needs – self audit for staff

## 1. Aims

The Great Learners Trust (GLT) aims to:

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

**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, radicalization, extremism and extreme sexual or physical violence
- **Contact** – being subjected to harmful online interaction with other users or generative AI applications that simulate this, 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), including those generated using AI, and online bullying
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

## 2. Legislation and guidance

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

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

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

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006, the Children's Wellbeing and Schools Act 2026 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.

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

## 3. Roles and responsibilities

### 3.1 The local governing board

The local governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training and monitor online safety logs as provided by the designated safeguarding lead (DSL).

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

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and that a review of the effectiveness of the filtering and monitoring systems is carried out by SLT at least once every academic year. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet their safeguarding needs

**All governors will**:

- Ensure that they have read and understand this policy

- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- 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) 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.

### 3.2 The headteacher

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

They will make sure that there are robust cover arrangements for when the DSL is unavailable due to illness, leave or other circumstances – for example, a confidential shared mailbox to make sure safeguarding concerns are received, monitored and acted on without delay.

### 3.3 The designated safeguarding lead (DSL)

Details of the school's DSL and deputy DSL 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 headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Ensuring that any online safety incidents are logged on the online safeguarding recording system and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary

- Providing regular reports on online safety in school to the headteacher and/or local governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

### 3.4 The ICT consultant

The ICT consultant role is provided by our ICT partner, Eduthing. They are 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 daily basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged on the online safeguarding recording system and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

### 3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware how to report any incidents by logging the incident on the online safeguarding recording system and following our child protection and safeguarding procedures
- Following the correct procedures by notifying the DSL and headteacher 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 on the online safeguarding recording system 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'

This list is not intended to be exhaustive.

### 3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher 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 (appendices 1 and 2)

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 – Help & advice | Childnet
- Parent resource sheet – Parents and Carers resource sheet (Childnet)

### 3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

## 4. Educating pupils about online safety

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

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

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 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 online 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 is shared and used online
- 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 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.

### 4.2 Pupils will be taught practical cyber security skills

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 physical security of devices
- 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 education on safeguarding issues such as cyber-bullying and the risks of online radicalisation.

## 5. 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.

The school will ensure parents are informed of the computing curriculum via the appropriate page on the school website. Children will access a range of online activity during their time at school. This will be monitored as outlined within this policy and anything they are directed to access will be age and content appropriate.

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 staff or the headteacher

# 6. Cyber-bullying

## 6.1 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 for learning policy.)

## 6.2 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. Class teachers will discuss cyber-bullying with their class groups.

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, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that 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 for learning 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.

## 6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for inappropriate images of files on pupils' electronic devices, including mobile phones iPads, and other tablet devices, where they believe there is 'good reason' to do so:

- It 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

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

- **Not** view the image*

- Confiscate the device and report the incident to the DSL immediately, who will report it to the police. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation in schools 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

*Staff will also never copy, print, share, store or save such images.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Assess how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher or DSL
- 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
- Ensure there is a witness present when viewing a device.

After conducting the search, the authorised staff member will document what happened and how they came to view the content.

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 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.

If inappropriate material is found on the device and 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. If the decision is made to delete the evidence this should be done in the presence of the child's parent. No staff will delete evidence.

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

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

For more detail, please refer to the GLT Searching, Screening and Confiscation Policy.

### 6.4 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.

The Great Learners Trust 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' or ‘deep nudes’, 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.

The Great Learners Trust will treat any use of AI to bully pupils very seriously in line with our behaviour for learning 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 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 staff.

Any use of artificial intelligence should be carried out in accordance with our AI usage policy.

## 7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school’s ICT systems and the internet (appendices 1 to 3). 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, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

## 8. Pupils using mobile devices in school

Please refer to the GLT Mobile Phone Policy.

In line with statutory guidance, our school is a mobile phone-free environment by default. Pupils are not permitted to have access to or use their mobile phones or smart technology with similar functionality to mobile phones (e.g. smart watches), which we refer to collectively as 'mobile phones', throughout the school day.

Any deviation from this mobile phone-free baseline will be by exception only (for example, approved arrangements for specific medical tracking) and must be explicitly authorised by the headteacher.

Where there is an arrangement by exception, any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

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

## 9. Staff using work devices outside 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 with strong passwords and multi-factor authentication. 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 – always install the latest updates
- Only using the Great Learners Trust (GLT) email address for work related communications.
- Ensure all emails containing sensitive or personal data sent outside the GLT are encrypted.

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used in accordance with our acceptable use policy.

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

## 10. 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 staff disciplinary procedures and code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

# 11. Training

## 11.1 Staff, governors and volunteers

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 the risks up
- 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 deputy DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

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

Volunteers will receive appropriate training and updates, if applicable.

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

## 11.2 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.

## 12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on the online safeguarding recording system

This policy will be reviewed annually by Trustees. At every review, the policy will be shared with the local governing 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.

## 13. Links with other policies

This online safety policy is linked to our:

- Child protection policy
- Behaviour for learning policy
- Conduct and discipline policy
- Data protection policy and privacy notices
- Complaints and resolutions policy
- ICT and internet acceptable use policy
- Mobile phone policy

## Appendix 1: Model acceptable use of the internet: agreement for parents and carers

| Acceptable use of the internet: agreement for parents and carers | |
|---|---|
| **Name of parent/carer:**<br><br>**Name of child:** | |
| Online channels are an important way for parents/carers to communicate with, or about, our school.<br>The school uses the following channels:<br>• Our official Facebook / Instagram accounts<br>• Email/text groups for parents (for school announcements and information)<br>• Our virtual learning platform<br>Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp). | |
| When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:<br>• Be respectful towards members of staff, and the school, at all times<br>• Be respectful of other parents/carers and children<br>• Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure<br><br>I will not:<br>• Use private groups, the school's Facebook / Instagram accounts, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way<br>• Use private groups, the school's Facebook / Instagram accounts, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident<br>• Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers | |
| **Signed:** | **Date:** |

## Appendix 2: Acceptable use agreement for KS2 pupils

**Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers**

**Name of pupil:**

**I will read and follow the rules in the acceptable use agreement policy**

**When I use the school's ICT systems (like computers and equipment) and get onto the internet in school**

**I will:**

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Only use generative AI in accordance with the trust's AI policy
- Always log off or shut down a computer when I'm finished working on it

**I will not:**

- Access any inappropriate websites including, but not limited to: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share any semi-nude or nude images, videos or livestreams, including anything created using AI, even if I have the consent of the person or people in the photo
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

**If I bring a personal mobile phone or other personal electronic device into school**:

- I will make sure it's switched off and handed in as required by school rules immediately upon entering the school
- I understand that I am not permitted to look at, use, or have access to my device at any point during the school day
- I will only use my device if I have official written permission from the school
- I agree that if I break the school rules on mobile devices, my device will be confiscated

| | |
|---|---|
| **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.** | |
| **Signed (pupil):** | **Date:** |
| **Parent/carer agreement:** I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these. | |
| **Signed (parent/carer):** | **Date:** |

## Appendix 3: Acceptable use agreement for EYFS and KS1 pupils

| **Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers** | |
|---|---|
| **Name of pupil:** | |
| **When I use the school's ICT systems (like computers and equipment) and get onto the internet in school…**<br><br>I will:<br>• Ask a teacher or adult if I can do so before using them<br>• Only use websites that a teacher or adult has told me or allowed me to use<br>• Tell my teacher immediately if:<br>  ○ I click on a website by mistake<br>  ○ I receive messages from people I don't know<br>  ○ I find anything that may upset or harm me or my friends<br>• Use school computers for school work only<br>• Be kind to others and not upset or be rude to them<br>• Not use them without asking a teacher first, or without a teacher in the room with me<br>• the school ICT equipment and tell a teacher straight away if something is broken or not working properly<br>• Only use the username and password I have been given<br>• Try my hardest to remember my username and password<br>• Never share my password with anyone, including my friends.<br>• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer<br>• Save my work on the school network<br>• Check with my teacher before I print anything<br>• Log off or shut down a computer when I have finished using it<br><br>**I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.** | |
| **Signed (pupil):** | **Date:** |
| **Parent/carer agreement:** I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these. | |
| **Signed (parent/carer):** | **Date:** |

## Appendix 4: Acceptable use agreement for staff, governors, volunteers and visitors

**Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors**

**Name of staff member/governor/volunteer/visitor:**

**When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, 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)
- Use them in any way which could harm the school's reputation
- Access social networking sites such as Facebook, Instagram, Twitter or chat rooms outside of the acceptable use policy.
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Input, upload, or process any personal data of pupils, confidential safeguarding information, or sensitive school data into public or unvetted generative AI tools (such as public AI chatbots or image generators). I will make sure I am aware of approved AI tools for use in school and follow this at all times
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

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 understand 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.

| **Signed (staff member/governor/volunteer/visitor):** | **Date:** |
|---|---|

## Appendix 5: online safety training needs – self audit for staff

| 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, governors and visitors? | |
| Are you familiar with the school's acceptable use agreement for pupils and parents/ carers? | |
| 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? | |