Hilderthorpe
PRIMARY SCHOOL
Aiming High ~ Reaching Higher

# E-Safety Policy

Policy Created: June 2020

Approved by Governors: June 2022

Policy Review Date: June 2024

**Contents**

## 1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

## 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
- 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 Department'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.

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

## 3. Roles and responsibilities

### 3.1 The governing board

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

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

The governor who oversees online safety is Richard Hare.

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)

### 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.

### 3.3 The designated safeguarding lead

Details of the school's DSL and deputy are set out in our child protection and safeguarding policy as well 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, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 5) 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 governing board

This list is not intended to be exhaustive.

### 3.4 Technical Support

The company designated as our Technical Support is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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 monthly basis or when it is deemed necessary.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) 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)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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.

### 3.6 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 - Childnet International
- Parent factsheet - Childnet International

### 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, when relevant, 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

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

We use Common Sense Media's e-safety scheme in each year group. From Y2 -6 each class will be taught one lesson per half term. EYFS and Y1, e- safety lessons are taught on a termly basis. We believe it is important to keep issues of e-safety fresh in the minds of our children, parents and staff. We invite parents to our e-safety lessons in order for them to engage with their children and learn more about the digital world we live in. This used in conjunction with the PSHE Jigsaw Scheme of Work that reinforces and supports these concepts. The safe use of social media and the internet will also be covered in other subjects where relevant.

- PHSCE and SRE in primary schools through the jigsaw programme

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

*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*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

## 5. 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.

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 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 tutor groups, and the issue will be addressed in assemblies. This will be addressed through our

e-safety lessons at some point during the year but can also be regularly with children in class discussion.

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 (Jigsaw Scheme of Work), 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 promotes information 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 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 consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

### 6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

## 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 1-3). 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.

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

**8. Pupils using mobile devices in school**

Pupils in UKS2 are permitted to bring a mobile phone into school, but this must be handed switched off and handed to the class teacher to be locked away. Phones may not be turned on until children have left the premises.

**9. Staff using work devices outside school**

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

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

Work devices must be used solely for work activities.

**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 within our acceptable use agreement. 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. 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**

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).

The DSL and deputy 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.

## 12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. A discussion following any incidents that require a wider whole school training/teaching response are acted upon collaboratively with the Computing leaders.

This policy will be reviewed annually by the Computing Leaders. At every review, the policy will be shared with the governing board.

## 13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Computing policy
- PHSCE/SRE policy

**Appendix 1: Children's acceptable use policy agreement**

# Hilderthorpe Primary School

Caring and Learning together for success

## Safety in a Digital World: Guide for Children and Young People

Digital technology opens up a world of entertainment, opportunity and knowledge. To help you stay safe this guide aims to provide information on:

- The benefits of Digital Technology
- Addressing the risks
- Further advice and support

The safety advice in this leaflet applies to all digital technology including computers, mobile phones, TVs, iPods, mass storage devices *etc*.

**The Benefits of Digital Technology**

You can use digital technology for many reasons, including:

**Finding and sharing information** – Researching topics on the internet, for school, college and for personal interests, and sharing media like files, pictures, films and music.

**Keeping in touch with family and friends** – Staying in touch with family and friends through Email, Instant Messaging (IM), Social Networking and chat rooms. Technology can be useful for contacting people in an emergency and making new friends in a safe way.

**Entertainment** – Listening to music, watching films, and playing interactive games.

**Shopping** – Buying items from companies and individuals all over the world, including online auctions.

**Addressing the risks: Digital technology agreement:**

There are however some risks in using digital technology – follow this advice and sign this agreement to help keep you safe.

**I agree to keep my personal information safe**

*Be careful what information you put on the internet and who can see it. Use a nickname online and privacy settings. This can help keep you safe.*

*Don't give out personal information like email addresses, home or school addresses or mobile phone numbers to people you do not know.*

*Only post photographs which you would be happy with your parents/carers seeing and make sure they don't show addresses. Photographs you post can be copied and sent to other people meaning you are not in control of them.*

*Do not share your passwords and log in details as people could access your information without your permission.*

**I will tell adults about the sites that I am worried about.**

**I agree not to meet people without asking a parent/carer/adult.**

*Some people on the internet are not who they say they are. Be careful who you chat to and make friends with on Social Networking or games sites. Never agree to meet someone without letting an adult know.*

**I agree to report and worries I have to an adult.**

*If anyone online makes you worried or says things that make you feel uncomfortable tell an adult or click 'Report abuse' button (some websites will ask you to download this first) and block them.*

*Do not respond to upsetting messages and cyber-bullying. Keep the message and show it to an adult you trust.*

**I agree not to use digital technology to bully people or make threats.**

*Cyberbullying is not acceptable and can cause distress.*

*Treat people as they would like to be treated.*

**Signed**..... **Date**.....

**Further advice and support:**

If you want to find out more about using digital technology safely go to:

www.thinkyouknow.co.uk Digital safety advice

www.ceop.gov.uk Report Abuse Button

Remember the internet safety code. Click Clever, Click Safe

- **Zip It** – Keep your personal stuff private and think about what you say and do online .
- **Block It** – Block people who send you nasty messages and don't open unknown links and attachments.
- **Flag It** – Flag up with someone you trust if anything upsets you or if someone asks to meet you online.

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

# Hilderthorpe Primary School

Caring and learning together for success

## Safety in a Digital World: Guide for Professionals

Technology is provided and maintained for the benefit of all staff within Hilderthorpe Primary School to enhance skills and become more effective in the workplace. You are encouraged to use and enjoy these resources, using the following agreement as a guide.

There is a need to ensure that digital technologies are used appropriately and for you to have an understanding of your responsibilities in keeping yourself and young people safe. This guide aims to assist you, making sure that you have all necessary measures in place.

**Internet and Email**

- **I agree to only access suitable material**;
  I am aware that accessing materials which are unlawful, obscene or abusive is not permitted.
- **I agree to report unsuitable material;**
  If I receive an email containing material of a violent, dangerous, racist, or inappropriate content, I will always report such messages to the E-safety Co-ordinator.
- **I agree to the professional code of behaviour;**
  I appreciate that other users might have different views from my own and acknowledge that the use of strong language or aggressive behaviour is not acceptable.
- **I agree to keep within copyright laws;**
  I will respect work and ownership rights of people, including abiding by copyright laws.
- **I agree to the responsible use of social networks, both within and outside the workplace;**
  The use of social networks for personal communication with children and young people for whom I am responsible is not appropriate.
- **I understand that misuse may result in disciplinary action**.

**Misuse**

Any identified misuse of the electronic mail facilities will be investigated and could result in action under the Council's Disciplinary policy and procedure.

Examples of misuse could include excessive personal or inappropriate use of the system, personal use during normal working hours, inappropriate use of the staff notice board facility, participation in chain/pyramid letters or similar schemes and initiating or forwarding messages which are abusive, defamatory or make improper or discriminatory remarks. The above list is not exhaustive.

(This policy should be read in conjunction with the corporate resources policy documentation - Policy and Guidelines on the use of Electronic Mail (Email)

**Equipment**

- **I agree to take care to protect hardware and software;**
  This includes protecting the ICT equipment from spillages by eating or drinking well away from them.

I will always get permission before installing, attempting to install or storing programs of any type on the ICT equipment. I will always check files brought in on removable media and mobile equipment (*e.g.,* laptops, PDAs *etc*) with antivirus software and only use them if they are found to be clean of viruses. I will only open attachments to emails if they come from someone I already know and trust. I understand that attachments can contain viruses or other programs that could damage files or software.

- **I agree to only using equipment within the context of my professional role;**
  I will only use ICT equipment for Hilderthorpe Primary School purposes. I understand that activities such as buying or selling goods are inappropriate.

**Security and Privacy**

- **I agree to take measures to protect access to data;**
  I will keep my log-on user name and password private, always log off when I have finished working or am leaving the ICT equipment unattended and regularly change my password (minimum of every 3 months). I am aware that I must never use someone else's user name. To protect myself and the systems, I will respect the security on the ICT equipment; I understand that attempting to bypass or alter the settings may put my work or other people's information at risk. I will not send sensitive information via non-secure email.

**Mobile phones**

- **I agree to always abide by Hilderthorpe Primary School policy for use of mobiles in the workplace;**
  I understand that the use of mobile phones for personal communication with children and young people for whom staff/volunteers have responsibility is not appropriate. Any such contact should be with the express permission of the Headteacher and recorded.

Staff are advised that any internet use can be monitored for appropriateness and volume of usage.

Name (print)……Signed……..……

Organisation……..…….....

Date ……

## Appendix 3: 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? | |
| 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? | |
| 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? | |