Online Safety Policy

Harvills Hawthorn Primary School

2022-2024

Reviewed May 2022

Introduction

This policy aims to outline the necessary procedures, behaviours and expectations which will improve the safety of children and staff in relation to the use of computers, mobile devices and any other technology.

We, as a school, recognise the growing concerns which are held by children, parents and educators about the risks and threats posed by technology which is, in many cases, readily available.

At Harvills Hawthorn Primary School, we have access to the internet through MacBooks, Windows computers, Chromebooks, iPads and will be getting Chrome Tablets in the near future. Therefore, this policy aims to ensure that these technologies and devices are used responsibly and safely to the end of ensuring safe use by staff and children alike.

This policy applies to all children, all staff, all volunteers/companies/visitors/students/educators and anyone else who may use technology within school.

This policy has been written by the Online Safety Co-ordinator (Ryan Brydon) and any safeguarding concerns, including those related to online safety, are dealt with by the headteacher and Designated Safeguarding Lead, Joanne Sheen.

This policy aims to address the ‘4 C’s’ of online safety, as outlined in the Keeping Children Safe in Education document. The 4 Cs are as follows

- Content
- Conduct
- Contact
- Commerce

Our online safety policy and curriculum endeavours to ensure both staff and children have an understanding of key safety advice, knowledge and information regarding each of these four areas.

Use of digital technologies, devices and the internet within school.

The use of digital technologies, devices and the internet should adhere to the following guidelines. Generally, usage should seek to promote education, learning and engagement and not stray into illegal or harmful usage which causes risk. The school expects all users of the technologies, devices and the internet to understand and follow the policy in order to establish a safe and purposeful basis in which computing and technology can be explored.

Users of the digital technologies, devices and internet within school should NOT:

- Visit internet sites, social media apps, make, post, download, upload or pass on material, comments or media which relates to:
    - Indecent images of children
    - Promoting discrimination of any kind
    - Promoting racial or religious hatred
    - Promoting illegal acts
    - Anything pornographic or sexual in nature
    - Anything which may cause offense to peers, staff or students

Sometimes, some of these areas may arise when exploring or browsing sites. When/if this happens, advise children (if they are involved) on how to deal with happening upon inappropriate material and later report the incident to the online safety co-ordinator, Mark Edwards, computer technician, or the designated safeguarding lead.
However, if there are incidents whereby deliberate access to websites, online forums or groups or articles which pertain to any of the following areas has been carried out, then the incident should be reported to the police:

- Images of child abuse
- Adult material which breaches the Obscene Publications Act
- Criminally racist or anti-religious material
- Violence and bomb making
- Illegal taking or promotion of drugs
- Software piracy
- Material related to terrorist activity or propaganda

In addition to this, users may also not use the school's broadband services in the following manners or instances:

- To run a private business
- Enter into personal transactions that involve the school
- Visit sites which may be defamatory or incur liability or adversely impact upon the image or reputation of the school or associated partners
- Use, upload, download or transmit copyrighted material
- Reveal confidential information, which includes but is not limited to: financial information, personal information, databases, computing access codes, business relationships.
- Intentionally interfere with the normal operation of the Internet connection
- Use the internet to reveal personal opinions which could be considered inappropriate or offensive
- Violate the privacy of others
- Corrupting or deleting others' data within prior permission
- Continue to use a device or item after request to desist because it is causing technical, safety, privacy or other issues
- Use technologies to intimidate, threaten or cause harm to others

- Use technology, either owned by the school or yourself, to take images or videos of children which are then taken out of the school premises (i.e. images or videos of children should not be stored on a device which will leave the school grounds).

Reporting abuse

- Any abuse suffered by children or staff should be reported to the SLT.
- Where possible, evidence (screenshots, recordings etc) should be kept and used to report the incident
- If the abuse is of a criminal nature, then it should, along with any relevant evidence, be reported to the police service.

Education and Training

We recognise the importance of a sound, thorough and purposeful education about the key elements of online safety relevant to the lives of the young people we teach. It is crucial that we ensure all children have an understanding of the risks posed by the use of online technologies, the consequences of their actions and decisions and the steps they can take to seek help, guidance and safety if instances occur which make them uncomfortable, anxious or fear for their or others' safety.

To this end, we ensure that online safety learning forms a crucial and paramount aspect of our computing curriculum. We have created a specific online safety curriculum which is based upon the document 'Education for a Connected World'. Each year group has a structured set of targets which will be taught throughout the academic year. These targets also specifically address each of the '4 C's' of online safety, as outlined in the Keeping Children Safe in Education document.

This curriculum will aim to teach children about various aspects of online safety, including teaching about how to use social media responsibly and to an age-appropriate level, about the dangers of cyberbullying and how to counteract it and about how 'sexting' can be damaging and dangerous (to an obviously age-appropriate level).

In order to deliver these targets effectively, teachers will be expected to deliver a class assembly, on a weekly basis, in relation to the targets outlined in their curriculum. Additionally, it is an expectation that key online safety messages are revisited each time teachers use technological equipment with their class. Furthermore, online safety is a key theme within our annual Safety Week and we also engage with Safer Internet Day as a school too. Therefore, children are exposed to a wealth of opportunity to learn, discuss and engage with online safety learning. Finally, through our RSHE and PSHE curriculum, we also deliver a Digital Wellbeing module for each year group every year, which also covers key aspects of the Online Safety Curriculum too.

In order for staff to deliver this wealth of online safety coverage adequately, they are frequently trained on new or topical online safety points. Every year, staff undertake safeguarding training and online safety forms part of this training. Also, at least once a year, staff receive explicit online safety training. Staff are made aware of practices, procedures, relevant information and where to find additional resources or information to further their knowledge.

As a school, we also understand the importance of educating and engaging with parents. We aim to provide updates on online safety issues through our distribution of newsletters or explicit communications, which inform parents of relevant issues. This is usually undertaken via e-mail or text message, whereby relevant threats, issues or knowledge are shared using produced materials, online links or information sheets. Much of this content comes from the platform, National Online Safety, which we subscribe to as a school in order to enable updated information and advice to accessed and distributed with ease and clarity.

Monitoring

The use of technology within school (by children) is always supervised by adults. As well as this ‘over the shoulder’ approach, all of our devices are equipped with forensic software, Impero, which is always scanning for key words which are identifiers for inappropriate or worrying use. If one of these key words is typed or searched for, a screenshot is taken and sent to Mark Edwards, along with the time of the incident. Mark Edwards will then investigate the incident and pass along any concerning information appropriately to the relevant people (SLT team, online safety co-ordinator, class teacher etc).

Sanctions

If a children is seen to be misusing technology or using technology in a way which is deemed worrying, concerning, harmful or abusive, then appropriate steps will be taken in line with the school’s behavior policy.

If the incident is serious enough in nature, the children’s parents will be informed and/or their use of technology may be suspended or withdrawn for their and others’ safety and wellbeing.

If staff are known, seen or proven to be misusing technology, then this shall be reported to the headteacher. If the staff are found to be in breach of any school policies, including this one, then disciplinary procedures may be undertaken. If the incident is serious in nature, then incidents may be passed to the police or child protection services.

It is important that all staff are responsible for their own actions but also for monitoring and reporting worrying actions witnessed by other members of staff to ensure the safety of all children and staff within school.

Remote Learning

Due to recent circumstances in regard to the coronavirus outbreak, we have had to put in place a system of remote learning to ensure that children can still access curriculum content, tailored by their teachers, at home. We have chosen to use the platform of Seesaw for this purpose.

Staff protecting themselves

- Staff must ensure they are only using Seesaw to communicate with children in appropriate ways and in a manner consistent with what would happen inside of school too. Staff should conduct themselves in accordance with the staff code of conduct policy at all times and maintain a professional relationship with children and parents.
- Staff should only 'contact' (be it through sending back work or comments) during school hours
- Staff should not engage in live video conversations with children where their parents are not readily available; where it is a 1:1 conversation or where they are the only adult on the video chat with a group of children.
- Staff must ensure that they report any safeguarding concerns they may have through the appropriate channels as normal, regardless of whether we are physically in school or not.
- Staff must ensure they have thoroughly checked all websites and videos they send to the children via Seesaw to verify they are appropriate and safe to access for young children.

Staff protecting children

- If staff have any concerns in relation to any comments made on Seesaw, any images/videos a child uploads or anything said during a phone call conversation, these should be reported in accordance with the safeguarding policy we have in place.
- Staff should contact the lead DSL (Joanne Sheen) in the first instance or any other DSL (Maxine Soper, Hayley Marsden, Kathryn Salmon, Josh Hill, Michelle Hellend, Hannah Kitching or Carla Eckersley) if Joanne Sheen is unavailable.
- Staff should be extra vigilant of mental health issues arising in children as potential 'lockdown' situations can be a difficult time for children and can place additional stress on families.

Children protecting themselves

- Staff should frequently deliver messages and provide resources to children about keeping safe online
- In the event that schools are closed in any future lockdowns, children will likely be using online technologies more than ever
- Therefore, key messages regarding benefits, dangers, help and support and length of time online must be given to children throughout the lockdown period. More advice on these messages can be sought online (see below) or from Ryan Brydon (Online safety lead).

- Children should be encouraged to respond positively, appropriately and respectfully to staff members and other children whilst online (both on Seesaw or on any other platform they may use independently from school).

Additional guidance

In England, the Department for Education (DfE) has published guidance on Safeguarding and remote education during coronavirus (DfE, 2020a).2 The DfE has also provided examples of remote education practice for schools during coronavirus (DfE, 2020b)3 and guidance on adapting teaching practice for remote education (DfE, 2020c).4

Advice can be found on the NSPCC website in regards to remote learning and how to keep safe online.
https://learning.nspcc.org.uk/news/2020/march/undertaking-remote-teaching-safely#heading-top