e-Safety and Cyberbullying Policy

CONVENTION ON THE RIGHTS OF THE CHILD

As a school that respects the rights of the children and adults in our school family, community and beyond, we aim for each school policy to adhere to articles from UNICEF's Convention on the Rights of the Child.

In this policy, we are working towards all of the articles.

Date Prepared: September 2023

Date Approved by Governing Body: September 2023

Date to be reviewed: September 2024

Little Hill Primary School

Policy on e-Safety and Cyberbullying

Introduction

Little Hill Primary School recognises the Internet and other digital technologies provide a vast opportunity for children and young people to learn. The Internet and digital technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning. As well as being a great tool for pupils, we recognise the increased risk to young people that the internet can pose including: child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm.

The nominated senior people for the implementation of the school's e-Safety policy are the e-Safety governor, e-Safety co-ordinator along with the senior leadership team.

Policy Statement

Little Hill's E-safety and cyberbullying policy was created in accordance with the DFE document 'Keeping Children Safe In Education' appendix 1.

The breadth of issues classified within online safety are considerable, but can be categorised into three areas of risk:

• content: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;

• contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and

• conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

In accordance with our policy, Little Hill strives to provide an education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children as well as the children themselves.

As part of our commitment to learning and achievement at Little Hill Primary School, we want to ensure that the Internet and other digital technologies are used to:

- Raise educational standards and promote pupil achievement.
- Develop the curriculum and enable the pupils to research safely using the Internet.
- Enable pupils to gain access to a wide span of knowledge in a way that ensures their safety and security.
- Enhance and enrich their lives and understanding.

To enable this to happen, we have taken a whole school approach to e-Safety which includes the development of policies and practices, the education and training of staff and pupils and the effective use of the school's ICT infrastructure and technologies.

Little Hill Primary School will ensure that the following elements are in place as part of its e-Safety and safeguarding responsibilities to pupils:

- A list of authorised persons who have various responsibilities for e-Safety.
- Information to parents that highlights safe practice for children and young people when using the Internet and other digital technologies.
- Adequate training for staff and volunteers.
- Adequate supervision of pupils when using the Internet and digital technologies.
- Education that is aimed at ensuring safe use of Internet and digital technologies.
- A reporting procedure for abuse and misuse.

Why is Internet Use Important?

Internet use is part of the statutory curriculum and is a necessary tool for learning.

It plays a major part of everyday life for education, business and social interaction today and therefore, the school has a duty to provide pupils with quality Internet access as part of their learning experience. Internet access is an entitlement for pupils who show a responsible and mature approach to its use.

Many pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security. The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

How Does Internet Use Benefit Education and Enhance Learning?

Benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and art galleries.
- Educational and cultural exchanges between pupils worldwide.
- Vocational, social and leisure use in libraries, clubs and at home.
- Access to experts in many fields for pupils and staff.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.
- Collaboration across networks of schools, support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.
- Access to learning wherever and whenever convenient.

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.

Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

When delivering lessons on e-Safety and cyberbullying staff will:-

- Be prepared to take disclosures and be confident about the Child Protection procedures.
- Be aware that children may be sensitive to the content owning to their own or other experiences and ensure appropriate support is available.
- Ensue curriculum information can be found on the website.
- Ensure that full coverage of the curriculum is taught in line with the National Curriculum requirements.

Use of Internet facilities, mobile and digital technologies

Little Hill Primary School will seek to ensure that Internet, mobile and digital technologies are used effectively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk. Breaches of an e-Safety policy can and have led to civil, disciplinary and criminal action being taken against staff, pupils and members of the wider school community. It is crucial that all settings are aware of the offline consequences that online actions can have. Schools must be aware of their legal obligations to safeguard and protect children on and offline and the accountability of these decisions will sit with the Head Teacher and the Governing body.

Little Hill Primary School expects all staff and pupils to use the Internet, mobile and digital technologies responsibly and strictly according to the conditions below. These expectations are also applicable to any voluntary, statutory and community organisations that makes use of the school's ICT facilities and digital technologies.

Users shall not visit Internet sites, including social networking sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children.
- Promoting discrimination of any kind.
- Promoting racial or religious hatred.
- Promoting illegal acts.
- Any other information which may be offensive to peers or colleagues e.g. abusive images; promotion of violence; gambling; criminally racist or religious hatred material.

Authorised Internet Access

World Wide Web

If staff or pupils discover unsuitable sites the URL (address) and content must be immediately logged with the ICT technician or SLT. Pupils must follow the procedure which is shared with all pupils by their class teacher.

The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Pupils will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work. The evaluation of on-line materials is a part of every subject.

Videoconferencing

IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.

All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.

- External IP addresses should not be made available to other sites.
- Videoconferencing contact information should not be put on the school website.
- School videoconferencing equipment should not be taken off school premises without permission. Use over the non-educational network cannot be monitored or controlled.

Videoconferencing should be supervised appropriately for the pupils' age and ability. Parents and carers consent should be sought for children to take part in videoconferences. Only key administrators should be given access to the videoconferencing system, web or other remote control page. Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference.

Recorded material shall be stored securely. If third-party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.

Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity. Establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site, it is important to check that they are delivering material that is appropriate for the class. Test links should be set up prior to the session. Teachers are responsible for ensuring the content is suitable for all pupils to access.

Social Networking

Pupil will be taught about age restrictions and recommendations for a variety of social networking tools. Children will also be explicitly taught the reasoning and purpose behind these restrictions.

Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.

Pupils will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the pupil or his/her location e.g. house number, street name or school.

Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others. Pupils will be advised not to publish specific detailed private thoughts including those of a negative nature.

Teachers' official blogs or wikis should be password protected and run from the school website. Teachers should be advised not to run social network spaces for pupil use on a personal basis. Newsgroups will not be made available unless an educational requirement for their use has been demonstrated.

School Website

There is to be a report abuse button on the Little Hill School's website that will link children and adults through to The Child Exploitation and Online Protection Unit site providing advice and links on how to report online abuse.

Filtering

Little Hill Primary School recognises that as part of its safeguarding responsibilities there is a need to work in partnership. One of our major partners is Openhive who provide the network, services and facilities and ensure filtering systems are as effective as possible, while allowing children to be taught the importance of self-regulation when using the Internet.

If staff or pupils discover unsuitable sites, the URL (address) and content must be immediately logged and a designated senior person informed.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Any material that the school believes is illegal must be referred to the DSL and ICT technician so that filters can be amended.

Filtering strategies will be selected by the school in discussion with the filtering provider where appropriate. Where possible, the filtering strategy will be selected to suit the age and curriculum requirements of pupils. The school's broadband access will include filtering appropriate to the age and maturity of pupils.

Managing Emerging Technologies

Little Hill Primary School is committed to ensuring that all its pupils will be able to use existing, as well as up and coming technologies, safely.

We are also committed to ensuring that all those who work with children and young people, as well as their parents, are educated as to the risks that exist so that they can take an active part in safeguarding children.

- Emerging technologies will be examined for educational benefit and a risk.

Publishing Images and Work

As part of the curriculum, photographs and video of children at work, on trips and with visitors are taken. The children are also taught to take photographs and videos, using school resources, of their own to use in their work, these often include their peers.

No images of pupils or staff will be published without prior consent and this consent is sought using the 'Parental Consent Form Using Images of Children' no work that the children have done will be published with their full name for data protection in accordance with GDPR 2018 laws.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the GDPR 2018 laws.

Handling e-Safety and Cyberbullying Complaints

Complaints about Internet misuse will be dealt with under the School's complaints procedure. Any complaint about staff misuse must be referred following the complaints procedure which is available to parents via the school website.

- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Any necessary sanctions will be decided upon using the school behaviour policy.

Communication of Policy

This policy will be communicated to all staff, at regular intervals, during Teacher Days and key messages from this policy will be delivered during E-Safety day and Anti-bullying week.

Staff

Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will need to be reported to the designated senior people, so that they can report it to the police:

- Images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative)
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist or anti-religious material
- Violence or terror related
- Illegal taking or promotion of drugs
- Software piracy
- Other criminal activity

Parents

Little Hill Primary School is committed to working in partnership with parents and carers and understands the key role they play in the Internet safety of their children, through promoting Internet safety at home and elsewhere.

We also appreciate that there may be some parents who are concerned about the use of the Internet, email and other digital technologies in school. In such circumstances, school staff will meet with parents and carers to discuss their concerns and agree upon a series of alternatives that will allow their child to fully access the curriculum, whilst remaining safe.

Cyberbullying

Cyberbullying can be defined as "Cyberbullying, or online bullying, can be defined as the use of technologies by an individual or by a group of people to deliberately and repeatedly upset someone else." (Childnet international, 2016- appendix 2). Many young people and adults find that using the internet and smart phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via smart phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

It is essential that young people, school staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety. There are a number of statutory obligations on schools, which Little Hill takes very seriously, with regard to all forms of behaviour which establish clear responsibilities to respond to bullying.

These measures link to the school's behaviour policy which is communicated to all pupils, school staff and parents. Where bullying outside school (such as online or via text) is reported to the school, it should be investigated and acted on. Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If school staff feels that an offence may have been committed they should seek assistance from the police.

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. There are clear procedures in place to support anyone in the school community affected by cyberbullying. All incidents of cyberbullying reported to the school will be recorded. There will be clear procedures in place to investigate incidents or allegations of cyberbullying. Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence using a bullying incident form or CPOMs.

The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary. The school will follow advice from the DFE document, 'Searching, screening and confiscation' (appendix 3) if they feel that a pupils personal device needs to be searched. Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.

Sanctions for those involved in cyberbullying will follow the schools procedures, such as:

- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.

- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.

Mobile Phones

The use of mobile phones and other personal devices by pupils in school is not allowed.

Use of mobile phones and other personal devices by staff in school should only be in their non-contact time and in accordance to the 'Authorised Acceptable Use Policy'. The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation. Mobile phones and personal devices will not be used during lessons or formal school time and therefore should be on silent at all times.

Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

Pupils Use of Personal Devices

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place until the end of the day.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members.

- Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Sexting

There is no clear definition of sexting, according to the Sexting in Schools document appendix 4, "Whilst professionals refer to the issue as 'sexting' there is no clear definition of 'sexting'. Many professionals consider sexting to be 'sending or posting sexually suggestive images, including nude or semi-nude photographs, via mobiles or over the Internet.'4 Yet when young people5 are asked 'What does sexting mean to you?' they are more likely to interpret sexting as 'writing and sharing explicit messages with people they know'.6 Similarly, many parents think of sexting as flirty or sexual text messages rather than images.7"

At Little Hill, through teaching of e-safety, we aim to ensure that pupils become aware of what sexting is, what to do if they become involved in a sexting incident and how to behave respectfully online.

The staff at Little Hill all receive safe-guarding training each year to ensure that they know what procedures to follow if an incident involving sexting occurs.

Radicalisation online

All members of staff at Little Hill are required to complete online training in order to support them in identifying, addressing and disclosing concerns around radicalisation online. Any concerns must be passed on to a DSL and logged using CPOMs.

Online grooming

Through e-safety and PHSE lessons children are taught all about the importance of keeping themselves safe online. They are taught the dangers of communicating with people that they don't know and keeping personal information safe. Teachers also receive safeguarding each year which includes identifying at risk pupils. Any concerns should be passes on to DSL and recorded on CPOMs.

Appendices

Appendix 1- Keeping children safe in education Statutory guidance for schools and colleges

Appendix 2- CYBERBULLYING: Guidance for schools

Appendix 3 - Searching, screening and confiscation

Appendix 4 - Reporting e-Safety Concerns Form