Policy 7H - Online Safety (previously) E-safety Policy
Including EYFS

(Review annually)

Date	Reviewed by	Date Reviewed by SMT	Date approved Sub-committee	Date approved Governors	Next review date
May 2023	Mrs C Goddings	06.06.2023	n/a	Category 3 Policy for 21st June 2023 Court meeting	May 2024 for June 2024 Bridewell Court Meeting

Category definitions

1. policies where there have been no changes
2. policies containing minor changes of a factual nature
3. policies which contain significant changes or are new and require thorough reading

Contents Page

1.0 POLICY AIMS

The E-safety Policy is part of The School Development Plan and relates to other policies including those for anti-bullying and cyberbullying (A8) and for child protection (A6).

- The E-safety committee key members are the E-safety Coordinator, The School's Designated Safeguarding Lead (DSL) and the Safeguarding Governor.
- The E-safety Coordinator is Mrs C Goddings.
- Our E-safety Policy has been written by the School, building on best practice and Government guidance.
- The E-safety Policy and its implementation will be reviewed annually.

The purpose of the Barrow Hills online safety policy is to:

- Safeguard and protect all members of the school community when using the internet.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

Barrow Hills identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:

content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-semitism, radicalisation and extremism.

contact: being subjected to harmful online interaction with other users; for example: child to child 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; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying);

We should also note the **commercialisation** of the online world with risks such as online gambling, phishing and or financial scams.

2.0 POLICY SCOPE

Barrow Hills believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all children and staff are protected from potential harm online. The school identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life. Barrow Hills believes that children should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all staff including the governing body, SMT, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as children, parents and carers.

This policy applies to all access to the internet and use of technology, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use offsite, such laptops, Chromebooks or mobile phones.

3.0 MONITORING AND REVIEW

Technology in this area evolves and changes rapidly. Barrow Hills will review this policy at least annually. The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure. We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied. To ensure they have oversight of online safety, the Head will be informed of online safety concerns, as appropriate. The named governor for safeguarding will report on a regular basis to the governing body on online safety practice and incidents, including outcomes. Any issues identified via monitoring will be incorporated into our action planning.

4.0 ROLES AND RESPONSIBILITIES

The Designated Safeguarding Lead (DSL) has responsibility for online safety. Barrow Hills also has an E-Safety Coordinator. However we recognise that all members of the community have important roles and responsibilities to play with regards to online safety.

<u>The Senior Management Team (SMT) team will:</u>

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff IT acceptable use policy, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all children to develop an age-appropriate understanding of online safety.
- Support the DSL and deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

<u>The Designated Safeguarding Lead (DSL) will:</u>

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside Deputy DSLs and E-Safety Coordinator to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.

- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date requirements to keep children safe online.

- Access regular and appropriate training and support to ensure they recognise the additional risks that children with SEN and disabilities (SEND) face online.

- Keep up to date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.

- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.

- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.

- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.

- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.

- Report online safety concerns, as appropriate, to the setting management team and Governing Body.

- Work with the SMT to review and update online safety policies on a regular basis (at least annually) with stakeholder input.

- Meet regularly with the governor with a lead responsibility for safeguarding and online safety.

<u>It is the responsibility of all members of staff to:</u>

- Contribute to the development of online safety policies.

- Read and adhere to the online safety policy and acceptable use policies.

- Take responsibility for the security of setting systems and the data they use or have access to.

- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.

- Embed online safety education in curriculum delivery, wherever possible.

- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.

- Identify online safety concerns and take appropriate action by following the setting safeguarding policies and procedure.

- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.

- Take personal responsibility for professional development in this area.

<u>It is the responsibility of staff managing the technical environment to:</u>

- Provide technical support and perspective to the DSL and SMT, especially in the development and implementation of appropriate online safety policies and procedures.

- Implement appropriate security measures including web filtering as directed by the SMT to ensure that the setting's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.

- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the SMT.

- Ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the SMT.

- Ensure appropriate access and technical support is given to the DSL (and/or Deputy) to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

<u>It is the responsibility of children (at a level that is appropriate to their individual age and ability) to:</u>

- Engage in age appropriate online safety education opportunities.

- Read and adhere to the acceptable use policies.

- Respect the feelings and rights of others both on and offline.

- Take responsibility for keeping themselves and others safe online.

- Seek help from a trusted adult, if there is a concern online.

<u>It is the responsibility of parents and carers to:</u>

- Read the acceptable use policies and encourage their children to adhere to them.

- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.

- Role model safe and appropriate use of technology and social media.

- Abide by the acceptable use policies.

- Identify changes in behaviour that could indicate that their child is at risk of harm online.

- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.

- Use our systems, such as learning platforms, and other network resources, safely and appropriately.

- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5.0 EDUCATION AND ENGAGEMENT POLICIES

Education and engagement with children:

A progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst children is in place.

- Ensuring education regarding safe and responsible use precedes internet access.

- Reinforcing online safety messages whenever technology or the internet is in use.

- Educating children in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.

- Teaching children to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Vulnerable children

Barrow Hills recognises that some children are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

The school will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable children and will seek input from specialist staff as appropriate.

Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.

- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates.

- This will cover the potential risks posed to children (Content, Contact and Conduct) as well as our professional practice expectations

- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.

- Make staff aware that their online conduct outside of school, including personal use of social media, could have an impact on their professional role and reputation.

Barrow Hills recognises that parents and carers also have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies. We will build a partnership approach to online safety with parents and carers by providing information and guidance on online safety in a variety of formats.

6.0 REDUCING ONLINE RISKS

Barrow Hills recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.

We will:

- Regularly review the methods used to identify, assess and minimise online risks.

• Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.

• Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.

Note: It is not possible to **guarantee** that unsuitable material cannot be accessed via school devices.

All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. Please see Appendices for further information.

7.0 SAFER USE OF TECHNOLOGY

7.1 Classroom Use

Barrow Hills children use chromebooks, the internet, which may include search engines and educational websites, learning platforms/intranet and email.

All school owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place. Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home. We will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community. We will ensure that the use of internet-derived materials, by staff and children, complies with copyright law and acknowledge the source of information.

Supervision of children will be appropriate to their age and ability.

Early Years Foundation Stage and Key Stage 1 - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the children' age and ability.

Key Stage 2 - children will use age-appropriate search engines and online tools. They will be directed by the teacher to online materials and resources which support the learning outcomes planned for the children' age and ability.

Key Stage 3 - children will be appropriately supervised when using technology, according to their ability and understanding

7.2 Managing Internet Access

We will maintain a written record of users who are granted access to our devices and systems. All staff and children will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet. School ICT systems security will be reviewed annually.

- School ICT systems security will be reviewed annually.
- Virus protection will be updated annually or as required if earlier.
- Security strategies will be discussed with Elmbrook Computers Ltd.
- Any security issues will be directed to Elmbrook by IT Support.

7.3 Filtering and Monitoring

School governors and leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learners' exposure to online risks. The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding. Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances. Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded. The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate. All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard children; effective classroom management and regular education about safe and responsible use is essential.

a)Filtering

Education broadband connectivity is provided through Elmbrook Computers Ltd. We use untangle which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature. The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.

If staff or children come across unsuitable on-line materials, the site must be reported to the E-Safety Coordinator.

The IT Department will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

b)Monitoring

We will appropriately monitor internet use on all school owned or provided internet enabled devices through physical monitoring (supervision) and active/pro-active technology monitoring services. If a concern is identified via monitoring approaches the DSL will respond in line with the Safeguarding policy. All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.4 Managing Personal Data Online

Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation. Full information can be found in our Data Protection policy (A21).

7.5 Security and Management of Information Systems

We take appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly.

• Encryption for personal data sent over the internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.

• Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.

• Not downloading unapproved software to work devices or opening unfamiliar email attachments.

• Regularly checking files held on our network,

• Specific user logins and passwords will be enforced for all but the youngest users.

• Where possible, for our most sensitive and important services accessible over the Internet, we use an additional means of authentication as well as a password, such as message to a mobile phone app

• All users are expected to log off or lock their screens/devices if systems are unattended.

7.6 Password Policy

All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private. From Year 3 all children are allocated their own unique username and private passwords to access our systems; children are responsible for keeping their password private. Below this age the E-Safety Coordinator will manage the passwords for the children. We require all users to:

• Use passwords for access into our system.

• Always keep their password private; users must not share it with others or leave it where others can find it.

• Not to login as another user at any time.

7.7 Managing the Safety of our Website

We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE). We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright. The administrator accounts for our website will be secured with an appropriately strong password. We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

When publishing images and videos online we will ensure that all images and videos shared online are used in accordance with the associated policies.

7.8 Managing Email

Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.

• The forwarding of any chain messages/emails is not permitted

• Spam or junk mail will be blocked and reported to the email provider.

• Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.

- Setting email addresses and other official contact details will not be used for setting up personal social media accounts.

Members of the community will immediately tell the DSL who will manage the concern either via safeguarding procedures or to the E-Safety Coordinator.

if they receive offensive communication, and this will be recorded in our safeguarding files/records. Excessive social email use can interfere with teaching and learning and will be restricted. Safeguarding issues will be sent to the DSL.

<u>Staff email</u>

The use of personal email addresses by staff for any official setting business is not permitted. Members of staff are provided with an email address to use for all official communication. Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, children and parents.

<u>Children's email</u>

From Year 3 children will use provided email accounts for educational purposes. Children will sign an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted. Whole-class or group email addresses may be used for communication outside of the setting.

7.9 Management of Applications (apps) used to Record Children's Progress

We use Tapestry, Google Workspace and our MIS (Engage) to track children' progress and share appropriate information with parents and carers. The Head is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation.

To safeguard learners' data:

- Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs.

- Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images.

- Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.

- All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.

- Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

8.0 SOCIAL MEDIA

The expectations regarding safe and responsible use of social media applies to all members of the Barrow Hills community. The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger. All members of the Barrow Hills community are expected to engage in social media in a positive, safe and responsible manner. All members of the Barrow Hills community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others. The use of social media during teaching/duty time for personal use is not permitted. Inappropriate or excessive use of social media during teaching/duty time hours or whilst using setting devices may result in disciplinary or legal action and/or removal of internet facilities. Concerns regarding the online conduct of any member of the Barrow Hills community on social media, should be reported to the DSL.

8.1 Staff Use of Social Media

The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities. Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the Acceptable Use Policy.

Reputation

All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting. Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities. All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):

- Setting the privacy levels of their personal sites.
- Being aware of location sharing services.
- Opting out of public listings on social networking sites.
- Logging out of accounts after use.
- Keeping passwords safe and confidential.
- Ensuring staff do not represent their personal views as that of the setting.

Members of staff are encouraged not to identify themselves as employees of Barrow Hills on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members. All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with our policies and the wider professional and legal framework. Information and content that staff members have access to as part of their employment, including photos and personal information about children and their family members or colleagues will not be shared or discussed on social media sites. Members of staff will notify the Senior Management Team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with children and parents and carers

All members of staff are advised not to communicate with or add as 'friends' any current or past children or their family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL (or deputy) and/or the Head. If ongoing contact with children is required once they have left the school, members of staff will be expected to use existing alumni networks or use official school provided communication tools. Staff will not use personal social media accounts to contact children or parents, nor should any contact be accepted, except in circumstances whereby prior approval has been given by the Head. Any communication from children and parents received on personal social media accounts will be reported to the DSL (or deputy).

8.2 Children's Use of Social Media

Safe and appropriate use of social media will be taught to children as part of an embedded and progressive education approach, via age appropriate sites and resources. We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for children under this age. Any concerns regarding children' use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour. Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.

Children will be advised:

- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
- Not to place personal photos on any social network space.
- To use nicknames and avatars when using social networking sites.
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- To use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications.
- How to report concerns both within the setting and externally.

9.0 USE OF MOBILE AND SMART TECHNOLOGY

9.1 Children's Use of Personal Devices and Mobile Phones

Barrow Hills recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff and parents/carers. Outside of school children have unlimited and unrestricted access to the internet via mobile phone networks which gives them access to harmful content and an opportunity to engage in harmful conduct. Within school however technologies need to be used safely and appropriately. All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies.

The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community; any breaches will be dealt with as part of our behaviour policy. All members of the school community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or safeguarding policy.

Children will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences. The school does not allow the use of personal mobile phones, other electronic devices, music players e.g. iPods, and handheld electronic games in school by children unless the Head has given specific permission. Any child who has to bring a phone to school should hand it in at the School Office and can collect it at the end of the school day. If a child is found in possession of an unauthorised personal device, it will be confiscated and passed to the Head of Organisation and Communication who will ensure its safety. A parent or legal guardian will have to request its return. Where there are safeguarding concerns, a member of staff reserves the right to ask children to unlock their device and search the contents.

9.2 Staff Use of Personal Devices and Mobile Phones

Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as: confidentiality, child protection, data security and acceptable use.

Staff will be advised to:

- Keep mobile phones and personal devices in a safe and secure place (List details e.g. locked in a locker/drawer) during lesson time.
- Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times and meetings.
- Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
- Not to use personal devices during lessons, unless written permission has been given by the Head, Deputy Head or Head of Pre-Prep, such as in emergency circumstances.
- Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.

Members of staff are not permitted to use their own personal phones or devices for contacting children or parents and carers.

- To take photos or videos of children and will only use work-provided equipment for this purpose.
- Directly with children and will only use work-provided equipment during lessons/educational activities. If a member of staff breaches our policy, action will be taken in line with our code of conduct
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or has committed a criminal offence, the police will be contacted.

10.0 RESPONDING TO ONLINE SAFETY INCIDENTS AND CONCERNS

All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.

All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns. Children, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

We require staff, parents, carers and children to work in partnership to resolve online safety issues.

After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required. If we are unsure how to proceed with an incident or concern, the DSL (or deputy) will seek advice from the Education Safeguarding Service. Where there is suspicion that illegal activity has taken place, we will contact the Education Safeguarding Service or Surrey Police using 101, or 999 if there is immediate danger or risk of harm.

The DSL (or deputy) will be informed of any online safety incidents involving safeguarding or child protection concerns. The DSL (or deputy) will record these issues in line with our safeguarding policy. The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant agencies. We will inform parents and carers of online safety incidents or concerns involving their child.

10.1 Online Sexual Violence and Sexual Harassment between Children

Barrow Hills recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation. Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our Safeguarding and Anti-Bullying policy.

Barrow Hills recognises that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities. We also recognise the potential for repeat victimisation in the future if abusive content continues to exist somewhere online. We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum. We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children. We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.

If made aware of online sexual violence and sexual harassment, we will:

- Immediately notify the DSL (or deputy) and act in accordance with our safeguarding and anti-bullying policies.

- Provide the necessary safeguards and support for all children involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- If appropriate, make a referral to partner agencies, such as Children's Social Work Service and/or the Police.
- If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
- If a criminal offence has been committed, the DSL (or deputy) will discuss this with Surrey Police first to ensure that investigations are not compromised.
- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

10.2 Youth Produced Sexual imagery (known as "sexting")

Barrow Hills recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).

We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people'. We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods. We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery. We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.

We will not:

- View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
- If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.
- Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request children to do so.

If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:

- Act in accordance with our safeguarding policy and the relevant county procedures.
- Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Store the device securely.
- If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.

- Carry out a risk assessment which considers any vulnerability of children involved; including carrying out relevant checks with other agencies.

- Inform parents and carers, if appropriate, about the incident and how it is being managed.

- Make a referral to Children's Social Work Service and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.

- Provide the necessary safeguards and support for children, such as offering counselling or pastoral support.

- Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.

- Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.

- Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.

- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary

10.3 Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

Barrow Hills will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

We recognise online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).

We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.

We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.

If made aware of an incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:

- Act in accordance with our Safeguarding policies and the relevant county procedures.

- If appropriate, store any devices involved securely.

- Make a referral to Children's Social Work Service (if required/appropriate) and immediately inform Surrey Police via 101, or 999 if a child is at immediate risk.

- Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).

- Inform parents/carers about the incident and how it is being managed.

- Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.

- Review the handling of any incidents to ensure that best practice is implemented; the leadership team will review and update any management procedures, where necessary.

We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment. Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/.

If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Service and/or Surrey Police. If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the DSL (or deputy). If learners at other settings are believed to have been targeted, the DSL (or deputy) will seek support from Surrey Police and/or the Education Safeguarding Service first to ensure that potential investigations are not compromised.

10.4 Indecent Images of Children (IIOC)

Barrow Hills will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC). We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site. We will seek to prevent accidental access to IIOC by using a filtering system which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti spam software. If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through Surrey Police and/or the Education Safeguarding Service.

If made aware of IIOC, we will:

- Act in accordance with our child protection policy and the relevant county procedures.
- Store any devices involved securely.
- Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Surrey police.

If made aware that a member of staff or a child has been inadvertently exposed to indecent images of children, we will:

- Ensure that the DSL (or deputy) is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Report concerns, as appropriate to parents and carers. If made aware that indecent images of children have been found on the setting provided devices, we will:
- Ensure that the DSL (or deputy) is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Inform the police via 101 (999 if there is an immediate risk of harm) and Children's Social Work Service (as appropriate).

- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- Report concerns, as appropriate to parents and carers.

If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:

- Ensure that the Head is informed
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations
- Quarantine any devices until police advice has been sought.

10.5 Cyberbullying

Cyberbullying, along with all other forms of bullying, will not be tolerated at Barrow Hills. Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

10.6 Online Hate

Online hate content, directed towards or posted by, specific members of the community will not be tolerated at barrow Hills and will be responded to in line with existing policies, including anti-bullying and behaviour. All members of the Barrow Hills community will be advised to report online hate in accordance with online safety and safeguarding policies. The Police will be contacted if a criminal offence is suspected. If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding Service and/or Surrey Police.

10.7 Online Radicalisation and Extremism

We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site. If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our safeguarding policy. If we are concerned that a member of staff may be at risk of radicalisation online, the Head will be informed immediately, and action will be taken in line with the safeguarding and allegations policies.

11.0 ONLINE SAFETY AWAY FROM SCHOOL

All staff will continue to look out for any signs that indicate a child may be at risk online and will report and respond to concerns in line with the child protection policy. Where necessary, referrals will be made to LADO. Children are encouraged to report concerns to a member of staff or a trusted adult at home.

Where this is not possible, additional support can be accessed online via:

- Childline: www.childline.org.uk
- UK Safer Internet Centre's 'Report Harmful Content': https://reportharmfulcontent.com
- National Crime Agency Child Exploitation and Online Protection Command (NCA-CEOP): www.ceop.police.uk/safety-centre

Parents/carers are encouraged to ensure children are appropriately supervised online and that appropriate parent controls are implemented. All communication with learners and parents/carers will take place using school provided or approved communication channels: for example, school provided email accounts, School Portal, Google Classrooms.

Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the DSL. Barrow Hills will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements. Staff and learners will engage with remote teaching and learning in line with existing behaviour principles as set out in our school behaviour policy.

12.0 NATIONAL LINKS AND RESOURCES

- CEOP: • www.ceop.police.uk
    - www.thinkuknow.co.uk • Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
- ChildLine: www.childline.org.uk
- Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk