**Barrow Hedges Primary School**

Policies and Procedures

**E-Safety Policy**

**This policy is part of the school’s Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school’s safeguarding and child protection processes.**

**Aims**

At Barrow Hedges Primary School, we aim 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 safe and responsible use of technology
* Establish clear mechanisms to identify and deal with incidents

**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 preventing and tackling bullying and guidance on protecting children from radicalisation. The policy takes into account the National Curriculum Computing programmes of study and PSHE recommendations. It also reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate content on pupils’ electronic devices, in line with the DfE’s advice for schools on searching, screening and confiscation.

**Roles and Responsibilities**

All governors will:

* Ensure that they have read and understood this policy
* Agree and adhere to the terms on acceptable use of the school’s ICT systems and the internet

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

 The Designated Safeguarding Lead (DSL) will:

* Work with the Headteacher, E-Safety Lead and other staff, as necessary, to address any online safety issues or incidents that have a child protection concern
* Liaise with other agencies and/or external services if necessary
* Provide regular reports on online safety in school to the Headteacher and/or governing board
* Pass on anonymous information about the types of incidents to the E-Safety Lead for staff training purposes and this will contribute to developments in policy and practice in online safety within the school

 The E-Safety Lead will:

* Update and deliver staff training on online safety and ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident
* Ensure that online safety education is embedded within the curriculum
* Ensure that online safety incidents are logged by the Designated Safeguarding Lead (DSL) and dealt with appropriately in line with this policy
* Ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school Behaviour Policy
* Communicate regularly with the Senior Leadership Team (SLT) to discuss current issues and review incident logs

Teachers will:

* Teach and embed the E-Safety curriculum as set out in the Computing and PSHE overviews
* Supervise and guide pupils carefully when engaged in learning activities involving online technology (including extra-curricular and extended school activities if relevant)

All staff and volunteers will:

* Read, ensure they understand, sign and adhere to the school Staff Acceptable Use Policy (AUP)
* Ensure that online safety incidents are dealt with and logged appropriately by the Designated Safeguarding Lead (DSL) in line with this policy and that they are reported to the E-Safety Lead
* Model safe, responsible and professional behaviours in their own use of technology

The ICT Service Manager is responsible for:

* Putting in place appropriate filtering, blocking and monitoring systems, which keep pupils safe from potentially harmful and inappropriate content and contact online whilst at school, including terrorist and extremist material
* Ensuring that the school’s ICT systems are secure and protected against viruses and malware

Parents are expected to:

* Ensure their child has read, understood and is adhering to the Pupil Acceptable Use Policy

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

UK Safer Internet Centre: [www.saferinternet.org.uk](http://www.saferinternet.org.uk)

 Childnet International: [www.childnet.com](http://www.childnet.com)

 NSPCC: <https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/>

 Net Aware: <https://www.net-aware.org.uk>

**Educating Pupils About Online Safety**

Pupils are specifically taught about safe use of the internet. Our policy is not to block everything and only allow pupils access to certain sites – they need to be taught what is acceptable and what is unacceptable, and what to do when they feel ‘uncomfortable’.

Through various teaching and learning opportunities, and as part of a broad and balanced curriculum, all pupils are made aware of online risks and taught how to stay safe online. Assemblies and guest speakers may also be used to educate pupils about the risks that can be encountered online. Pupils are taught about safeguarding issues, including how technology can provide a platform for issues such as child sexual exploitation, radicalisation and sexual predation. Pupils are taught about the safe use of social media and, using age-appropriate resources, are taught how to stay safe from radicalisation, Child Sexual Exploitation, FGM, grooming and peer-on-peer abuse. We use the curriculum to ensure that children and young people understand how people with extreme views share these with others, especially using the internet. Pupils are equipped with the skills needed to feel safe and adopt safe online practices to help them recognise online risks and stay safe from abuse.

Pupils in EYFS and Key Stage 1 are taught:

* To use technology safely and respectfully, keeping personal information private
* To 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 are taught:

* To use technology safely, respectfully and responsibly
* To recognise acceptable and unacceptable behaviour
* To identify a range of ways to report concerns about content and contact

The breadth of issues classified with online safety 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.

**Cyber-bullying**

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.

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 themselves 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 a victim.

Emotional abuse may involve serious bullying (including cyberbullying), causing children frequently to feel frightened or in danger, or the exploitation or corruption of children.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour Policy. The DSL and E-Safety Lead 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.

**Safeguarding**

The first indication of concern about a pupil’s welfare is not necessarily the presence of an injury. Signs that could be an indication of abuse may include:

* Misuse of information technology (e.g. Youth Produced Sexual Imagery, inappropriate comments on Social Media, texting, cyberbullying and online grooming)

**Monitoring and Filtering**

When pupils use the school's network to access the internet, they are protected from inappropriate content by our filtering and monitoring systems. However, some pupils are able to access the internet using their own data plan (e.g. if a child in Year 6 brings in their mobile phone – see below about mobile phones). To minimise inappropriate use, pupils are supervised and guided carefully when engaged in learning activities involving online technology. Online safety education is embedded within the curriculum and pupils are taught how to use online technology safely and responsibly. The school will ensure that the use of filtering and monitoring systems does not cause ‘over blocking’ which may lead to unreasonable restrictions as to what pupils can be taught regarding online teaching.

**Email**

All staff use LGfL’s Staffmail for email, and all pupils use LGfL’s Londonmail for email. Both systems have virus and malware scanning on every email, as well as ‘rude word’ checking, etc. Any emails found to exceed the threshold (set at ‘3’) are flagged up and reported to the authorised users. Authorised users have the ability to look at any emails within both systems. Other webmail systems are blocked.

**Examining electronic devices**

School staff have the specific power under the Education and Inspections Act 2006 and 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 a member of the Senior Leadership Team to decide whether they should:

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

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

**Mobile phones**

Only children in Year 6 are able to have a mobile phone in school. If they choose to bring a mobile phone into school it must be left with the class teacher for the duration of the school day. If the phone is used inappropriately the child will not be able to bring the device into school again, as signed for in the Acceptable Usage Policy. It is the child’s responsibility to hand their phone in to their class teacher. The school takes no responsibility for loss or theft. Mobile phones will be kept securely and returned before the end of the day.

**Acceptable Use of the Internet**

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 (see appendices). 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.

More information is set out in the acceptable use agreements in the appendices.

**Responding to Issues of Misuse**

Clear processes are in place to identify and deal with incidents effectively. All pupils, parents and staff sign an Acceptable Usage Policy.

Where a pupil misuses the school’s ICT systems or the internet, the action taken will depend on the individual circumstances, nature and seriousness of the specific incident. We will follow the procedures set out in the Behaviour Policy and/or the following:

* Incidents will be reported to the E-Safety Lead and DSL
* The Designated Safeguarding Lead will pass on anonymous information to the E-Safety Lead and this will contribute to developments in policy and practice in online safety within the school
* Where pupils have breached the Acceptable Use Policy, they will fill in a Behaviour Pupil Reflection sheet (as set out in the Behaviour Policy)
* Parents/Carers will be informed of online safety incidents involving children for whom they are responsible
* The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the appropriate authorities – police, Internet Watch Foundation, CEOP

Incident forms are monitored by the E-Safety Lead and any learning points are used to develop staff training, pupil education or parent awareness e.g. specific lessons are taught relating to the breach; external speakers are invited in to speak about specific topics; additional parent workshops are held for a particular year group etc.

**Training**

All staff members will receive training, including refresher training, at least once every academic year, on safe internet use and online safeguarding issues including cyber-bullying and risks of online radicalisation. They will receive relevant updates as required, e.g. through emails and staff meetings. All staff members will be made aware of the following:

* Pupil attitudes and behaviours which may indicate that they are at risk of potential harm online.
* The procedure to follow when they have a concern regarding a pupil’s online activity.

**Staff use of mobile phones and cameras**

* Staff will not use personal mobile phones or cameras when pupils are present.
* Staff may use mobile phones on school premises outside of working hours when no pupils are present.
* Staff may use mobile phones during breaks and non-contact time as long as no children are present.
* Staff will use their professional judgement in emergency situations.
* Staff may take mobile phones on trips, but they must only be used in emergencies and should not be used when pupils are present.
* Personal mobile devices will not be used to take images or videos of pupils or staff in any circumstances.
* The school have provided devices for staff to take photos.
* The sending of inappropriate messages or images from mobile devices is strictly prohibited.
* Staff will adhere to the E-Safety Policy at all times.
* Photographs and videos of pupils will be carefully planned before any activity with particular regard to consent and adhering to the school’s Data Protection Policy.
* Where photographs and videos will involve LAC pupils, adopted pupils or pupils for whom there are security concerns, a member of the Senior Leadership Team will liaise with the Designated Safeguarding Lead to determine the steps involved. The DSL will, in known cases of a pupil who is a LAC or who has been adopted, liaise with the pupil’s social worker, carers or adoptive parents to assess the needs and risks associated with a pupil.
* Staff will report any concerns about another staff member’s use of mobile phones to the Designated Safeguarding Lead.

**Related Policies**

This E-Safety policy is linked to our Child Protection and Safeguarding, Behaviour and Safe Working for Practice agreement. It also takes accounts for the media consent that parents have given for their child/children.

**Appendix 1: Acceptable Use Agreement (Parents/Carers)**

At Barrow Hedges Primary School, we ensure that all pupils have good access to digital technologies to support their teaching and learning and we expect all our pupils to agree to be responsible users in order to keep everyone safe.

At school your child will be asked to read (or will have read to them) and sign an Acceptable Use Policy Agreement tailored to his/her age. Please read this carefully – it is attached in Appendix 2 or 3.

I understand that my child has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

As the parent/carer of the pupil below, I understand that my son/daughter will have access to the internet and to ICT systems at school and is expected to follow the Acceptable Use Policy Agreement.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that children will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that the school takes inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour. I understand that my child’s activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy Agreement.

I understand that only children in Year 6 are able to have a mobile phone in school. If I choose for my child to bring a mobile phone into school because I wish them to have this on their journey to and from school, it must be left with the class teacher for the duration of the school day. I understand that it is my child’s responsibility to hand their phone in to their class teacher and that the school takes no responsibility for loss or theft. I understand that if the phone is used inappropriately, my child will not be able to bring the device into school again.

I will support the school by promoting safe and responsible use of the internet, online services and digital technology at home and will inform the school if I have concerns.

I understand that if I take photographs or videos at school events that have other children or staff in them, I will not share these online without their permission.

Name(s) of pupil(s): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Child’s Class: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Parent/Carer Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Parent /Carer Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Appendix 2: Pupil Acceptable Use Policy Agreement EYFS and Key Stage 1**

This agreement will help keep me safe and help me to treat others respectfully.

**This is how I will keep safe online:**

|  |  |
| --- | --- |
| I will only use the devices and websites my teacher says I’m allowed to use.  |  |
| I will check before I use new sites, games or apps.  |  |
| I will remember that people online aren't always who they say they are and will not arrange to meet them.  |  |
| I won’t change clothes in front of a camera or send photos of myself or others.  |  |
| I won’t share my personal information (including my name, address, telephone number, usernames, passwords, religion, ethnicity or health information).  |  |
| I will be kind and polite to people online and will not join in with bullying.  |  |
| I will tell a trusted adult if I am worried, scared or just not sure.  |  |

Child’s Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Child’s Class: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Appendix 3: Pupil Acceptable Use Policy Agreement Key Stage 2**

This agreement will help keep me safe and help me to treat others respectfully.

**In order to stay safe online I must remember:**

***I am an online digital learner –*** I will use the school’s internet and devices for schoolwork and learning activities. I will only use sites, games and apps that my trusted adults say I can.

***I am secure online –*** I will not share my password with others or log in using someone else’s details. I will not open any attachments in emails, or follow any links in emails, without first checking with a teacher.

***I am private online –*** I will not give out my personal information (including my name, address, telephone number, usernames, passwords, religion, ethnicity or health information). I will never change what I wear in front of a camera and won't send photos of myself or others.

***I am a rule-follower online –*** I know that some websites and social networks have age restrictions and I respect this. I will not use the internet without a teacher being present or without their permission, and will only visit sites that my trusted adults have agreed to.

***I am respectful online –*** I will not post, make or share unkind, hurtful, rude or inappropriate messages or materials and will tell my trusted adults if I see these. I will not join in with cyber-bullying or sharing of inappropriate material. I will not use inappropriate language when communicating online.

***I am responsible online –*** I will tell a trusted adult if I find material or messages that might upset, distress or harm myself or others or if someone is being bullied online. I will not access or share inappropriate materials, websites, social networking sites or chat rooms.

***I am careful online –*** I will not arrange to meet anyone offline without asking a trusted adult. I understand that unless I have met someone in real life, I can’t be sure who someone is online.

I understand that if I breach the rules, I may not be allowed to use the internet for a period of time as determined by my teacher. I will also take part in an E-Safety reflection session where I will discuss appropriate use of the internet, watch videos or take part in additional learning activities based on the breach I took part in. My teacher will help me fill in a reflection sheet during the activity saying what I have learned about how to behave online in future.

I have read and understood this agreement.

Child’s Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Child’s Class: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Appendix 4: Acceptable Use Agreement (Staff, Governors, Volunteers and Visitors)**

When using the school’s ICT systems and accessing the internet in school, or outside school on a work device:

* I will not browse, access, or attempt to access, inappropriate material, including but not limited to material for a violent, criminal or pornographic nature or material that is considered offensive or of an extremist nature by the school.
* I will not support or promote extremist organisations, messages or individuals.
* I will not use any improper language when communicating online, including in emails or other messaging services.
* I will not install any unauthorised software.
* I will not engage in any online activity that may compromise my professional responsibilities.
* I understand that I have a responsibility to uphold the standing of the teaching profession and of the school, and that my digital behaviour can influence this.
* I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school’s most recent online safety and safeguarding policies.

**Mobile phone and camera safety**

I have read and understand that:

* I will not use personal mobile phones or cameras when pupils are present.
* I may use mobile phones on school premises outside of working hours when no pupils are present.
* I may use mobile phones during breaks and non-contact time as long as no children are present.
* I may take mobile phones on trips, but they must only be used in emergencies and should not be used when pupils are present.
* Personal mobile devices cannot be used to take images or videos of pupils or staff in any circumstances.
* The school have provided devices for staff to take photos.
* The sending of inappropriate messages or images from mobile devices is strictly prohibited.
* Photographs and videos of pupils will be carefully planned before any activity with particular regard to consent and adhering to the school’s Data Protection Policy.
* Where photographs and videos will involve LAC pupils, adopted pupils or pupils for whom there are security concerns, I will speak to a member of the Senior Leadership Team and/or Designated Safeguarding Lead to determine the steps involved.
* I will report any concerns about another staff member’s use of mobile phones to the Designated Safeguarding Lead.
* I will adhere to the E-Safety Policy at all times.

I will only use the school’s ICT systems and internet for educational purposes or for the purposes of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit.

I will let the E-Safety Lead or Designated Safeguarding Lead (DSL) know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school’s ICT systems responsibly, and will ensure that pupils in my care do so too.

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_