**Online Safety Policy**

**Policy Statement**

For clarity, the Online Safety policy uses the following terms unless otherwise stated:

**Users** - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

**Parents** – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

**School** – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

**Wider school community** – students, all staff, governing body, parents and any other stakeholders.

Safeguarding is a serious matter; at Barham Primary School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

* To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
* To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the Barham Primary School website; upon review all members of staff will sign as read and understood both the Online Safety policy and the Staff Acceptable Use Policy. A copy of this policy and the Students Acceptable Use Policy will be sent home with students at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.

**Policy Governance (Roles & Responsibilities)**

**Governing Body**

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

* Review this policy at least annually and in response to any Online Safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure Online Safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
* Appoint one governor to have overall responsibility for the governance of Online Safety at the school who will:
* Keep up to date with emerging risks and threats through technology use.
* Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.
* Chair the Online Safety Committee

**Headteacher**

Reporting to the governing body, the Headteacher has overall responsibility for Online Safety within our school. The day-to-day management of this will be delegated to a member of staff, the Online Safety Officer (or more than one), as indicated below.

The Headteacher will ensure that:

* Online Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
* The designated Online Safety Officer(s) has had appropriate CPD in order to undertake the day to day duties.
* All Online Safety incidents are dealt with promptly and appropriately.

**Online Safety Officer**

The day-to-day duty of Online Safety Officer is devolved Natalie Tyndale

The Online Safety Officer will:

* Keep up to date with the latest risks to children whilst using technology; familiarize him/herself with the latest research and available resources for school and home use.
* Review this policy regularly and bring any matters to the attention of the Headteacher.
* Advise the Headteacher, governing body on all Online Safety matters.
* Engage with parents and the school community on Online Safety matters at school and/or at home.
* Liaise with the local authority, IT technical support and other agencies as required.
* Retain responsibility for the Online Safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
* Ensure any technical Online Safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
* Make him/herself aware of any reporting function with technical Online Safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

**ICT Technical Support Staff**

Names: Paulette Williamson (Technical Support) and Sumit Parmar (Network Manager)

**All Staff**

Staff are to ensure that:

* All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
* Any Online Safety incident is reported to the Online Safety Officer (and an Online Safety Incident report is made), or in his/her absence to the Headteacher. If you are unsure the matter is to be raised with the Online Safety Officer or the Headteacher to make a decision.
* The reporting flowcharts contained within this Online Safety policy are fully understood.

**All Students**

The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

Online Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school.

**Parents and Carers**

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents evenings, parent open days, school newsletters, the school website and the MLE the school will keep parents up to date with new and emerging Online Safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

**Online Safety Committee**

Chaired by the Governor responsible for Online Safety, the Online Safety Committee is responsible:

* to advise on changes to the Online Safety policy.
* to establish the effectiveness (or not) of Online Safety training and awareness in the school.
* to recommend further initiatives for Online Safety training and awareness at the school.

Established from volunteer students, parents, Online Safety Officer, responsible Governor and others as required, the Online Safety Committee will meet on a termly basis.

**Technology**

Barham Primary School uses a range of devices including PC’s, laptops and iPads. In order to safeguard the students and in order to prevent loss of personal data we employ the following assistive technology:

**Internet Filtering** – we use London Grid for Learning (LGfL) and ‘Symantic’ Endpoint Protection software that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The ICT Coordinators, Online Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

**Email Filtering** – we use the London Grid for Learning that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

**Encryption** – All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner’s Office.

**Passwords** – all staff and students will be unable to access any device without a unique username and password (with the exception of iPads). Staff and student passwords will change on a regular basis or if there has been a compromise, whichever is sooner. The ICT Coordinator and IT Support will be responsible for ensuring that passwords are changed.

**Anti-Virus** – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns. All USB peripherals such as key drives are to be scanned for viruses before use.

**Safe Use**

**Internet** – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this Online Safety and the staff Acceptable Use Policy; students upon signing and returning their acceptance of the Acceptable Use Policy.

**Email** – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted. Students are permitted to use the school email system, and as such will be given their own email address. The email address will be made up of their first name and a two-figured number, e.g. john09@barham.brent.sch.uk

**Photos and videos** – Digital media such as photos and videos are covered in the schools’ Photographic Policy, and is re-iterated here for clarity. All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance.

**Social Networking** – there are many social networking services available; Barham Primary School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within Barham Primary School and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the Online Safety Officer who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

* Blogging – used by staff and students in school.
* Twitter – used by the school as a broadcast service (see below).

A broadcast service is a one-way communication method in order to share school information with the wider school community.

In addition, the following is to be strictly adhered to:

* Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
* There is to be no identification of students using first name and surname; first name only is to be used.
* Where services are “comment enabled”, comments are to be set to “moderated”.
* All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner’s permission has been granted or there is a license which allows for such use (i.e. creative commons).

**Notice and take down policy** – should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

**Incidents** - Any Online Safety incident is to be brought to the immediate attention of the Online Safety Officer, or in his/her absence the Headteacher. The Online Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an **Online Safety incident log**.

**Training and Curriculum** - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Barham Primary School will have an annual programme of training which is suitable to the audience.

Online Safety for students is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student’s learning. At Barham, ICT is at the forefront of all subjects and activities in our school, for this reason we recognise the need for all pupils to be taught to use the internet efficiently and safely, and develop a responsible and mature approach to accessing and interpreting information. We also recognize that that the internet can benefit the professional work of staff and enhances the school’s management information and business administration systems, so staff have to be equally educated in the appropriate use of the internet and its resources.

At Barham, we take the issues surrounding Online Safety very seriously. Online Safety is embedded in all we do throughout our school. We believe that it is important to teach children about Online Safety in the same way we teach about road, water and cycle safety. Our school network is filtered and maintained by a talented ICT team who work together in keeping our network secure and free from viruses and other inappropriate material. Children are presented with many activities to challenge their thinking and to encourage safe practices whilst using ICT/Computing, Internet, mobile phones and other forms of digital resources. And to have the confidence to report any issues including cyberbullying to an adult they trust.

At Barham we have created a safe ICT learning environment that includes 3 main elements:

* An effective range of technological tools
* Policies and procedures, with clear roles and responsibilities
* A comprehensive Online Safety (Digital Citizenship & Technology) education programme for pupils, staff and parents through the use of a range of resources such as LGFL Online Safety teaching resources, Think U Know, CEOP Internet Safety videos and the PitDa (Parenting in the Digital Age) programmes).

As well as these programmes of training we will establish further training or lessons as necessary in response to any incidents.

The Online Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Headteacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

The Online Safety Training Programme can be found – *In the Computing Folder in the Trainee Head’s Office*

**Online Safety Incident Log**

|  |  |  |
| --- | --- | --- |
| **Number**: | **Reported By:** *(name of staff member)* | **Reported To:** *(e.g. Head, Online Safety Officer)* |
|  | **When:** | **When:** |
| **Incident Description:** (Describe what happened, involving which children and/or staff, and what action was taken) |
| **Review Date:** |  |
| **Result of Review:** |
|  |
| **Signature (Headteacher)** |  | **Date:** |  |
|  |
| **Signature (Governor)** |  | **Date:** |  |

**Risk Log**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **No.** | **Activity** | **Risk** | **Likelihood** | **Impact** | **Score** | **Owner** |
| 1. | Internet browsing | Access to inappropriate/illegal content - staff | 1 | 3 | 3 | Online Safety OfficerIT Support |
| 1. | Internet browsing | Access to inappropriate/illegal content - pupil | 2 | 3 | 6 |  |
| 2. | Blogging | Inappropriate comments | 2 | 1 | 2 |  |
| 3. | Blogging | Using copyright material | 2 | 2 | 4 |  |
| 4. | Student laptops | Access to inappropriate/illegal content - pupil | 1 | 2 | 3 |  |
| 5. | Student iPads | Access to inappropriate/illegal content - pupil | 1 | 2 | 3 |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**Likelihood: How likely is it that the risk could happen (foreseeability).**

**Impact: What would be the impact to the school (e.g. this could be in terms of legality, reputation, complaints from parents, reporting in press etc.)**

**Likelihood and Impact are between 1 and 3, 1 being the lowest.**

**Multiply Likelihood and Impact to achieve score.**

**LEGEND/SCORE: 1 – 3 = Low Risk**

 **4 – 6 = Medium Risk**

 **7 – 9 = High Risk**

**Owner: The person who will action the risk assessment and recommend the mitigation to Headteacher and Governing Body.**

 **Final decision rests with Headteacher and Governing Body**

**Inappropriate Activity Flowchart**

Consider:

Risk assess

Counselling

Discipline

Referral

**Report to Designated Safeguarding Leader JJ &**

**E-Safety Officer NT**

**Report to**

**ESafety Officer,**

**Risk assess &
Inform parents**

**Report to Designated Safeguarding Leader & ESafety Officer**

No

Yes

Yes

No

Child Protection Issue?

Child Protection Issue?

Pupil

Member of Staff

Who is involved?

A concern is raised

**Illegal Activity Flowchart**

If you are in any doubt, consult the Esafety Officer, Headteacher, Safeguarding Leader or Brent LSCB

**Report to**

**ESafety Officer &**

**Headteacher**

Report to:
Brent

LSCB

0208 937 4300

Report to:
Brent

LSCB

0208 937 4300

Report to:

Safeguarding

Leader

Brent LSCB

0208 937 4300

Report to:

Police

020 87333189

Brent LSCB

Tel: 01223 567243

Note: NEVER investigate

 NEVER show to others for your own assurance

 DO NOT let others handle evidence – Police only

Secure evidence in locked storage.

Inform Parents

E-Safety Officer

Inform Designated Safeguarding

Leader JJ

Yes

No

Child Protection Issue?

Pupil

Member of Staff

Who is involved?

A concern is raised