Horsley  School

**E-Safety Policy**

***Online safeguarding, known as e-safety is an area that is constantly evolving.***

***We use technology and the internet extensively across all areas of the curriculum***

***and have done all that is possible to ensure children are protected.***

**Purpose and Aims**

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 school website; upon review all members of staff will sign as read and understood both the e-safety policy and the Staff Acceptable Use Policy. A copy of this policy and the Students Acceptable Use Policy will be sent home with new students at the beginning of the 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.

For clarity, the e-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,

This policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

Headteacher Name: Lisa Brind Signed:

Chair of Governors: Mark Kelly Signed:

Review Date: 1 September 2014

**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 e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-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 e-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.
* establish the effectiveness (or not) of e-safety training and awareness in the school.
* to recommend further initiatives for e-safety training and awareness at the school.

**Headteacher**

Reporting to the governing body, the Headteacher has overall responsibility for e-safety within our school. The day-to-day management of this will be the responsibility of the Headteacher and Computing Subject Leader.

They will ensure that:

* E-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 e-Safety Officers have had appropriate CPD in order to undertake the day to day duties.
* All e-safety incidents are dealt with promptly and appropriately.

**E-Safety Officer**

The day-to-day duties of an e-Safety Officer are the responsibility of the Computing Subject Leader.

The e-Safety Officer will:

* Keep up to date with the latest risks to children whilst using technology; familiarise 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 e-safety matters.
* Engage with parents and the school community on e-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 e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail is in place.
* Ensure any technical e-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 e-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**

Technical support staff are responsible for ensuring that:

* The IT technical infrastructure is secure; this will include at a minimum:
	+ Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
	+ Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
	+ Any e-safety technical solutions such as Internet filtering are operating correctly.
	+ Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and Headteacher.
	+ Passwords are applied correctly to all adult users
	+ The IT System Administrator password is to be changed on a monthly (30 day) basis.

**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 e-safety incident or potential e-safety incident is reported to the e-Safety Officer (and an e-Safety Incident report is made), or to the Headteacher.
* The reporting flowcharts contained within this e-safety policy are fully understood.

**All Children**

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.

E-Safety is embedded into our curriculum through lessons, assemblies and discussion; students will be given the appropriate advice and guidance by staff. Similarly all children 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 and school newsletters the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered. It is recommended that parents use the internet at home with their child, develop a similar set of rules and invest in appropriate security software.

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 Children’s Acceptable Use Policy before any access can be granted to school ICT equipment or services.

**Technology**

Horsley Church of England Primary School uses a range of devices including PC’s, laptops, and Nexus tablets. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

**Internet Filtering** – we use RM SafetyNet Plus supplied by SWGfL 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 Computing Subject Leader 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 RM EasyMail security that prevents any infected email being sent from the school, or received by 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 using either encryption software or hardware. 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 will be unable to access any device without a unique username and password. IT Support will be responsible for ensuring that passwords are changed regularly.

**Anti-Virus** – All capable devices will have anti-virus software. This software will be updated 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 keydrives 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 e-safety and the Staff Acceptable Use Policy; to children upon signing and returning their acceptance of the Student Acceptable Use Policy. Children will not pursue internet research without staff supervision and the free use of search engines is not permitted.

**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. Children do not have individual email addresses.

**Photos and videos** – Digital media such as photos and videos are covered in the Use of Photographic Images consent form, and is re-iterated here for clarity. All parents must sign a photo/video release slip; non-return of the permission slip will not be assumed as acceptance. Any images of children will not be labeled with their names and will only appear on the website if parents have agreed to this.

**Social Networking** – Currently social media services are not used by the school, with the exception of the Friends of Horsley School Facebook and Twitter accounts. Prior to the use of any social media services by Horsley Church of England Primary School there will be a full risk assessment. If staff wish to use social media, permission must first be sought via the e-Safety Officer/Headteacher for a decision to be made.

**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 e-safety incident is to be brought to the immediate attention of the e-Safety Officer, or in his/her absence the Headteacher. The e-Safety Officer will assist in taking the appropriate action to deal with the incident and to fill out an 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, Horsley Church of England Primary School will have an annual programme of training which is suitable to the audience and any additional training found necessary as a result of e-safety incidents or other instigators.

E-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. Progressive discrete e-safety lessons are taught throughout the school with additional emphasis during Anti-bullying and Healthy Living or E-safety weeks. Extra lessons are to be taught in response to e-safety incidents or changes.

The GCC E-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.

 Horsley  School

Acceptable Use Policy – Staff

**Note: All Internet and email activity is subject to monitoring**

You must read this policy in conjunction with the E-Safety Policy. Once you have read and understood both you must sign this policy sheet

**Internet access** - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-safety incident, reported to the e-safety officer and an incident sheet completed.

**Social networking** – is allowed in school in accordance with the e-safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become “friends” with parents or pupils on personal social networks

**Use of Email** – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

**Passwords** - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student, or IT support.

**Data Protection** – If it is necessary for you to take work home, or off site, you should ensure that your device (laptop, USB pendrive etc.) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

**Personal Use of School ICT** - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries of personal use.

**Images and Videos** - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

**Use of Personal ICT** - use of personal ICT equipment is at the discretion of the Headteacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support and the e-Safety Officer.

**Viruses and other malware** - any virus outbreaks are to be reported to SWGfL as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

**E-Safety** – like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of ICT whether you are with other members of staff or with students.

**NAME :**

**SIGNATURE : DATE :**

 Horsley  School

Acceptable Use Policy – Children

**Our Charter of Good Online Behaviour**

**Note: All Internet and email activity is subject to monitoring**

**I promise** – to only use the school ICT for schoolwork that the teacher has asked me to do.

**I promise** – not to look for or show other people things that may be upsetting.

**I promise** – to show respect for the work that other people have done.

**I will not** – use other people’s work or pictures without permission to do so.

**I will not** – damage the ICT equipment, if I accidentally damage something I will tell my teacher.

**I will not** – use other people’s usernames or passwords.

**I will not** – share personal information online with anyone.

**I will not** – download anything from the Internet unless my teacher has asked me to.

**I will** – let my teacher know if anybody asks me for personal information.

**I will** – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

**I will** – be respectful to everybody online; I will treat everybody the way that I want to be treated.

**I understand –** that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

**I understand** – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

**Signed (Parent) :**

**Signed (Student) :**

**Date :**

**Monitoring**

* All staff, students and parents of students will be informed that Internet activity may be monitored in order to ensure as much as possible that users are not exposed to illegal or inappropriate websites, and to ensure as much as possible that users do not actively seek access to illegal or inappropriate websites.
* Staff must understand why monitoring is important, be allowed to voice any concerns and set their expectations of how the data can be used.
* A letter is sent home to parents, explaining that the Internet activity may be monitored, and why, to be distributed alongside the Acceptable Use Form.

*Note: users must be informed of monitoring, but consent is not required.*

 Horsley  School

Dear Parent/Guardian,

**Use of the Internet**

Use of the internet in school is a vital part of the education of your son/daughter. Our school makes good use of the internet in order to enhance their learning and provide facilities for research, collaboration and communication.

You will be aware that the internet is host to a great many illegal and inappropriate websites, and as such we will ensure as far as possible that your child is unable to access sites such as this. We are able to do this using advanced software known as an internet filter. This filter categorises websites in accordance with their content; the school allows or denies these categories dependent upon the age of the child, through SWGfL – South West Grid for Learning.

The software also allows us to monitor internet use; the internet filter keeps logs of which user has accessed what internet sites, and when. Security and safeguarding of your child are of the utmost importance in our school; in order to ensure that there have been no attempts of inappropriate internet activity we may occasionally monitor these logs. If we believe there has been questionable activity involving your child we will inform you of the circumstances.

At the beginning of each school year we explain the importance of internet filtering to your child. Furthermore we explain that there has to be a balance of privacy and safety; we also inform them that we can monitor their activity. All children are given the opportunity to ask questions and give their viewpoint. We would like to extend that opportunity to you also; if you have any questions or concerns please contact either Miss Heathcote or myself.

We would like you to discuss the Charter of Good Online Behaviour (see overleaf) with your child. Please return your signed copy to school. We realise that some of these items will not apply to our youngest children but we wanted you to be aware of what we consider to be ‘Acceptable Use’.

Yours sincerely

Lisa Brind

Headteacher

**Use of the Internet**

I have read this letter and understand that my child’s Internet access could be monitored to ensure that there is no illegal, or inappropriate activity by any user of the school network. I acknowledge that this has been explained to my child and that he/she has had the opportunity to voice their opinion, and to ask questions. I accept responsibility for setting standards for my child to follow when selecting, sharing and exploring information and media at home.

Name of Child – Name of Parent/Guardian –

Signature - Date

**E-Safety Incident Log**

|  |  |  |
| --- | --- | --- |
| **Number**: | **Reported By:** *(name of staff member)* | **Reported To:** *(e.g. Head, e-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**

(with a couple of examples)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **No.** | **Activity** | **Risk** | **Likelihood** | **Impact** | **Score** | **Owner** |
| 1. | Internet browsing | Access to inappropriate/illegal content - staff | 1 | 3 | 3 | e-Safety OfficerIT Support |
| 1. | Internet browsing | Access to inappropriate/illegal content - students | 2 | 3 | 6 |  |
| 2. | Blogging | Inappropriate comments | 2 | 1 | 2 |  |
| 2. | Blogging | Using copyright material | 2 | 2 | 4 |  |
| 3. | Student laptops | Students taking laptops home – access to inappropriate/illegal content at home | 3 | 3 | 9 |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**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 Bod**

**Risk Assessment**

|  |  |
| --- | --- |
| **Risk No.** | **Risk** |
| 3 | In certain circumstances, students will be able to borrow school-owned laptops to study at home. Parents may not have internet filtering applied through ISP. Even if they do there is no way of checking the effectiveness of this filtering; students will potentially have unrestricted access to inappropriate/illegal websites/services. As the laptops are owned by the school, and the school requires the student to undertake this work at home, the school has a common law duty of care to ensure, as much as is reasonably possible, the safe and well being of the child. |
| LIkelihood | The inquisitive nature of children and young people is that they may actively seek out unsavoury online content, or come across such content accidentally. Therefore the likelihood is assessed as 3. |
| 3 |
| Impact | The impact to the school reputation would be high. Furthermore the school may be held vicariously liable if a student accesses illegal material using school-owned equipment. From a safeguarding perspective, there is a potentially damaging aspect to the student. |
| 3 |
| Risk Assessment | HIGH (9) |
| Risk Owner/s | e-Safety OfficerIT Support |
| Mitigation | This risk should be actioned from both a technical and educational aspect:Technical: Laptop is to be locked down using XXXXXXXX software. This will mean that any Internet activity will be directed through the school Internet filter (using the home connection) rather than straight out to the Internet. The outcome is that the student will receive the same level of Internet filtering at home as he/she gets whilst in school. Education: The e-Safety Policy and Acceptable Use Policy will be updated to reflect the technical mitigation. Both the student and the parent will be spoken to directly about the appropriate use of the Internet. Parents will be made aware that the laptop is for the use of his/her child only, and for school work only. The current school e-safety education programme has already covered the safe and appropriate use of technology, students are up to date and aware of the risks. |

**Approved / Not Approved (circle as appropriate) Date:**

**Signed (Headteacher) : Signed (Governor) :**

**Inappropriate Activity Flowchart**

If you are in any doubt, consult the Headteacher or Designated Safeguarding Lead

Report to:

GCSB

and/or

Police

Report to:

GCSB

and/or

Police

Consider:

Risk assess

Counselling

Discipline

Referral

Consider:

Inform parents

Risk assess

Counselling

Discipline

Referral

Report to Headteacher

No

Yes

Yes

No

Child Protection Issue ?

Child Protection Issue ?

Pupil

Member of Staff

Who is involved?

A concern is raised

**Illegal Activity Flowchart**

Report to Headteacher and

Designated Safeguarding Lead

Report to Headteacher and Designated Safeguarding Lead

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

Refer to Police

Inform Safeguarding

Yes

No

Child Protection Issue ?

Pupil

Member of Staff

Who is involved?

A concern is raised

Report to:

Police

and

GCSB

Report to:

GCSB

and

Police