Holymead Primary School

E-Safety Policy

1. Aims

1.0 Holymead Primary School aims to provide the children with a computing & PSHE curriculum that develops them as safe internet users. We aim to provide a stimulating learning experience, through all subjects that enables the children to become confident internet users. We encourage an open dialogue about internet use with children, parents, carers and school staff.

2. Rationale

2.0 The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail. Computer skills are vital to access life-long learning and employment; indeed computing is an essential life-skill.

2.1 Schools have an important role to play in equipping children to stay safe online both inside and outside school. Therefore e-safety education will be incorporated into the computing and PSHE curriculum.

2.2 Most technologies present risks as well as benefits. Internet use for work, home, social and leisure activities is expanding in all sectors of society. This brings young people into contact with a wide variety of influences, some of which – as in life generally – may be unsuitable. It is important that schools, libraries and youth clubs, as well as parents, adopt strategies for the safe and responsible use of the Internet.

2.3 The Curriculum, Standards and Inclusion committee will review, monitor and update Internet use and E-safety education, through the use of SWGfL 360Safe review tool, reviewing incidents and procedures and pupil conferencing.

3. How will E-safety be taught in lessons?

Pupils will be regularly taught how to protect themselves online using the SMART rules displayed in all classrooms and computer rooms. They will also have dedicated E-safety sessions as part of the computing scheme of work using the SWFGL lessons.

Pupils will supervised when using the internet and clear age related learning objectives will be shared for efficient, safe internet research and learning.

Communications (including passwords) will be taught through the computing curriculum and PSHE:

- Children will use simulated email or the class blogs (see blogging policy) where all posts can be monitored by teachers, to ensure that they can apply SMART rules in a safe simulated environment.
- Children will discuss only communicating online with people who they know in real life e.g. friend or family. This is particularly important before joining group chats or group games out of school.

- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to identify and manage online advertising and how to close “pop-ups” or additional advertising tabs/windows.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- The evaluation of on-line materials is a part of teaching/learning in every subject.
- Pupils will access online resources, such as CBBC Newsround where they can evaluate content reliability, check the validity of the information and acknowledge the source to respect copyright.
- Teachers will use planning guidance “Digital Literacy” [www.digital-literacy.org.uk] provided from SWGFL to ensure progression of the safety skills across the key stages.

4. Managing information

4.0 How will information systems security be maintained? Passwords

- Access to confidential files and SIMS database is password protected through an individual user’s login that has enhanced rights over a child’s login. Passwords will be set to a high level of security, and SIMS passwords will be different to teacher’s laptop password. ICT technician, email administrator and E-Safety Leader will ensure passwords are changed when and if necessary.
- The school business manager and bursar have administrator rights to the school website and email.
- The Blogging leader and E-Safety leader has administrator rights to the blog site.
- Passwords should not be disclosed to anyone verbally or by email.
- No laptops should be left unattended without locking the screen (Including lunch time and after school)
- All devices and websites (e.g. blog and TTRockstars) should be logged out after use.
- Children reminded to not save their passwords on school technology and log out after use.
- The school website will be protected by year group passwords.
- All teachers are expected to close SIMs when not in use.

4.1 How will e-mail be managed?

- Access in school to external personal e-mail accounts will be blocked to children and may be blocked to staff.
- Pupils may only use approved apps and virtual learning environments that are simulated or where posts are approved / monitored by the teacher. Inappropriate apps will be blocked as soon as the E-Safety leader is made aware of the new apps as and when they are developed.
- Pupils must immediately tell a teacher if they receive offensive message/e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication or other social network messaging, such as address or telephone number, or arrange to meet anyone.
- USB flash drives and portable hard drives will not be used to store data. All data will be stored on the server and teacher laptops (Password protected)

4.2 How should published website content be managed?

- The School Business Manager, Administrator & Senior Leadership team will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The Web site should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

4.3 Can pupil's images or work be published?

- Pupil full names will not be used anywhere on the Holymead website
- Pupil work can only be published with their permission (For blogging see the separate policy)

4.4 How will social networking, social media and personal publishing be managed?

- Pupils and staff will not be allowed access to public or unregulated chat rooms and social networks during school time (The exception to this is Twitter – see blogging Policy).
- The school will BLOCK access to social media and social networking sites.
- During e-safety assemblies, computing and PSHE lessons, pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Staff follow the Bristol City Council, code of conduct on use of social networking sites.
- In addition, teachers will follow the DfE Teachers' Standards

4.5 How will emerging technologies be managed?

- Emerging technologies (such as tablets) will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. (See appendix of E-Safety risk assessment)
- Mobile phones will not be used on site without express permission of the head teacher (see Acceptable Use of Mobile Phones Policy)
- Communications between the school and parents/carers via text messaging are monitored by the head teacher.
- All communications should use school texting system/school office staff, and not personal mobile phones.

5. Internet Access

5.1 How will Internet access be authorised?

- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents and pupils will be asked to read and sign a user agreement when their child first joins the school.
- Pupils will not be issued individual email accounts; e-mailing will take place in a simulated environment, or through a teacher controlled, monitored email system using a generic email address through the SWGFL scheme of work.
- Staff laptops have an extra layer of rights so that YouTube or QuietTube can be accessed on their laptops. This is managed through our filtering systems and server permissions by the IT technician.

5.2 How will the risks be assessed?

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly through the governor committees.
- The headteacher and Curriculum, Standards and Inclusion committee will ensure that the Internet policy is implemented and compliance with the policy monitored.
- The E-safety risk assessment will be reviewed annually, or informed by events from Bristol City Council IT, media or SWGFL (South West Grid for Learning).

5.3 How will filtering be managed?

- The ICT Technician will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The school will use the Bristol L.A. filtering system on the broadband connection and 'allow lists' restricts access to a list of approved sites.
- **The strict filtering of content prevents children from accessing internet chat rooms or web pages where radical or terrorist extremist material is could be encountered.**
- **When using the internet, school staff should continue to monitor internet use to ensure pupils are not accessing material that is likely to contain extremist or terrorist material - e.g. news articles, links from other websites that may get through the filtering process.**
- The school will work in partnership with Bristol L.A. to ensure systems to protect pupils are reviewed and monitored.
- If staff or pupils discover unsuitable sites, the URL must be reported to the ICT Leader/Technician/Headteacher
- Any material that the school believes is illegal must be referred to the CEOP and/or Internet Watch Foundation.
- Any member of staff, may contact Professionals Online Safety Helpline **0344 3814772** for advice on any e-safety incident.

5.4 How will Cyber bullying be managed?

- Cyber bullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's policy on anti-bullying.
- All incidents of cyber bullying reported to the school will be investigated and recorded.

- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence (copies of offensive messages or screen shots).
- The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in Cyber bullying include:
    - The bully will be asked to remove any material deemed to be inappropriate or offensive.
    - A service provider may be contacted to remove content.
    - Internet access may be suspended at school for the user for a period of time.
    - Access to school systems will be blocked
    - Parent/Carers will be informed.
    - The Police will be contacted if a criminal offence is suspected.

6. Communications

6.0 How will the policy be introduced to pupils & parents?

- Rules for Internet access will be posted in all rooms where computers are used.
- Parents and Pupils will agree to the schools Acceptable Use Policy in September.
- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- Assemblies about e-safety and Participation in Safer Internet Day organised nationally.
- The school website will contain a page advising parents of ways for their children to Stay Safe online
- E-safety taught as part of computing and PSHE, as well as reguarly referred to SMART rules when pupils are using the internet on computers, laptops or iPads or other device.

6.1 Staff conduct using technology

- All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school.
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet & E-safety Policy, and its importance explained.
- All staff should closely monitor internet use within their classroom and the ICT suite.
- All staff report any E-safety incidents in the E-safety book.

6.2 How will complaints regarding Internet use be handled?

- Pupils and parents will be informed of the complaints E-safety reporting procedure (See Appendix 1 flow diagram).
- Parents and pupils will need to work in partnership with the E-safety leader and Head teacher to resolve issues.
- Responsibility for handling incidents will be delegated to the E-safety leader, Family Link Worker and/or Designated Safeguarding Lead.
- Any complaint about staff misuse must be referred to the Headteacher, or Chair of Governors.

7. Performance Indicators

The effectiveness of e-safety education will be judged by the designated e-safety governor, chair of the curriculum, standards and inclusion committee. Pupil conferencing sessions will be held to judge pupils' understanding of how to keep personal information safe and appropriate online behavior using the SMART rules.

The school will be judged on its overall progress in Internet and E-safety through the use of SWGfL 360 Safe self review tool.

8. Role of E-safety Leader

The E-safety leader will:

- Keep up to date on developments
- Investigate e-safety incidents, following school procedure, reporting to the head teacher and inclusion committee.
- Ensure participation in national internet safety events (Safer Internet Day)
- Providing all members of staff with guidelines to show how aims are to be achieved and how the variety of all aspects of e-safety is to be taught
- Advising on in-service training to staff where appropriate. This will be in line with the needs identified in the School Development Plan and within the confines of the school budget.
- Report to the Curriculum, Standards and Inclusion committee.

9. Monitoring

This policy, e-safety procedures, e-safety incidents will be monitored by the Governors' Curriculum, Standards and Inclusion committee. Please see Governing body terms of reference.

Other Relevant Policies / Documents

E-safety risk assessment
School's Acceptable Use Policy (based on SWGfL)
School's Laptop Policy
School's Use of Mobile Phones Policy
Governor's Terms of Reference for Inclusion committee
E-safety incident book
E-safety incident flow chart
Blogging Policy

Date: June 2018

To be revised: June 2019

Rights Respecting School Article 24

You have the right to a safe environment

Appendix 1

E-safety incident flow chart

Switch off screen, close laptop or turn off whiteboard	
Accidental	Deliberate

↓

Record incident in E-safety book
Head Teacher, Designated Safeguarding Lead/Deputy, E-safety Leader or member of Senior Leadership team investigate incident and record information (including screen shots / printout as evidence)

↓

Report abuse / request removal of material
Esafety Leader / School Business Manager / Provider for School Website Vysiion (IT systems support): 01249 446500 Bristol Schools IT Helpdesk: 0117 90 37999 Schools Internet Team (contact using above number) Professional Online Safety Helpline 0344 3814771

↓

In School Action – Who is involved?			
Child Arrange meeting with Parent/Carer	**Parents/Carer** Request meeting / send letter	**Staff** Governing body / HR and/or Police	**Volunteer/Other** Request meeting / contact police

↓

Apply Sanctions
Child protection or anti-bullying procedures followed, written warning, restrict or ban use of school IT systems, accounts closed at source, use report button (social networks), staff disciplinary procedures.

↓

Report to Governors for review			
Review policies and procedures	Report in the Internet Watch Foundation and SWGFL	Review schools IT systems	Identify support for victim