Holymead Primary School

E-Safety Policy

1. Aims

1.0 Holymead Primary School aims to provide the children with a computing & PSHC 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.

1.1 Rights Respecting School Article 24: You have the right to a safe environment

2. Rationale

2.0 Holymead Primary School 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 material
- **Contact:** being subjected to harmful online interaction with other users
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

2.1 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 online learning platforms and content. Computer skills are vital to access life-long learning and employment; indeed, computing is an essential life-skill.

2.2 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 PSHC curriculum.

2.3 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/Carers adopt strategies for the safe and responsible use of the Internet.

2.4 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?

3.0 Pupils will be regularly taught how to protect themselves online using the class E-safety charters and SMART rules displayed in all classrooms and computer rooms. They will also have dedicated termly E-safety sessions as part of the computing scheme of work using: Sharp, Alert Secure, Kind and Brave (Google, 2020), Digital Literacy (SWGfL, 2020).

The curriculum overview and E-safety tracker will record the clear age related learning objectives and will be monitored by the E-Safety lead.

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.
- School business manager will monitor access and use of information, referring GDPR policy.
- The school business manager and bursar have administrator rights to the school website, online platforms and email.
- The Computing, E-Safety leader, SLT and School Business Manager has administrator rights to online learning platforms.
- 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. online learning platforms) 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 contact be managed?

- Staff will use the Holymead Office email address to contact parents/carers if required, not their individual work account
- Access in school to external personal e-mail accounts will be managed for staff through our filtering access for adults and blocked to children. Staff should follow the Code of Conduct.
- **Staff and Visitor Mobile phones will not be used within sight or hearing of pupils and should be switched to silent during the school day.** (see Acceptable Use of Mobile Phones Policy)
- Pupils may only use approved apps and virtual learning environments where posts are approved / monitored by the teacher.
- Inappropriate apps or websites will be blocked if needed, by E-safety Lead / ICT technician
- Pupils must immediately tell a trusted adult if they receive offensive messages / posts on any device.
- Pupils must not reveal personal details of themselves or others in communication or posts online, such as address or telephone number, or arrange to meet anyone (see E-safety charter).

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 Website 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 or online learning platforms.
- Pupil work can only be published with their permission
- The office holds a central list of pupils who cannot have their photo published, class teachers and SLT to monitor.

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 school filtering system will block access to social media and social networking sites.
- Staff may have access via their own device / 4G connection but follow Code of Conduct
- Pupils will follow Mobile Phone Policy and leave personal devices at the office.
- During e-safety assemblies, computing and PSHC lessons, pupils will be advised never to give out personal details of any kind which may identify them and / or their location.
- Staff follow the Bristol City Council, code of conduct and DfE Teachers' Standards

4.5 How will emerging technologies be managed?

- Emerging technologies and apps will be examined for educational or administration benefit and a risk assessment will be carried out before use in school is allowed. (See appendix of E-Safety risk assessment)

5. Internet Access

5.1 How will Internet access be authorised?

- Parents/Carers will sign an Acceptable use Policy and pupils sign the E-safety charters (every September) to access to monitored and filtered internet access.
- Pupils will be issued with individual usernames and passwords for online learning platforms
- Staff laptops have different filtering to allow access to websites, such as YouTube. This is managed through our filtering systems and server permissions by the ICT technician.

5.2 How will the risks be assessed?

- 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).
- 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 E-safety risk assessment and monitored by the headteacher and Governors, Curriculum, Standards and Inclusion committee.
- The headteacher and Curriculum, Standards and Inclusion committee will ensure that the E-safety policy is implemented and compliance with the policy monitored.

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.
- If staff or pupils discover unsuitable sites, the URL must be reported to the ICT Leader/ICT Technician/Headteacher and reported Bristol IT and/or CEOP/Internet Watch Foundation.
- Any member of staff, may contact Professionals Online Safety Helpline 0344 3814772 or helpline@saferinternet.org.uk 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
    - Parents/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/carers?

- Rules for Internet access will be posted in all rooms where computers are used.
- Pupils will sign the E-safety charter displayed in classrooms
- Parents/Carers and Pupils will agree to the schools Acceptable Use Policy on joining the school.
- Instruction in responsible and safe internet use should precede any internet access.
- The will school will have assemblies about e-safety and participate in Safer Internet Day every February
- The school website will contain a page advising Parents/Carers of ways for their children to Stay Safe online
- E-safety is taught as part of computing and PSHC curriculum

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 E-safety Policy, and its importance explained.
- All staff should closely monitor internet use within their classroom and the Computer suite.
- All staff report any E-safety incidents in the Behaviour book/CPOMS/ICT Technician Log.

6.2 How will complaints regarding Internet use be handled?

- Pupils and parents/carers will be informed of the complaints E-safety reporting procedure (See Appendix 1 flow diagram).
- Parents/Carers 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. 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.

8 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact for e-safety / safeguarding
- Ensure that online safety is promoted to parents/carers and the wider community through a variety of channels and approaches.
- Liaise with other members of staff, such as pastoral support staff, E-safety leader, ICT technician and the SENCO on matters of online safety.
- The DSL will ensure online safety is recognised as part of the safeguarding responsibilities, and that a coordinated whole school approach is implemented.
- Monitor online safety incidents to identify gaps and trends and use this data to update the education response and school policies and procedures.

9. Monitoring

This policy, e-safety procedures, e-safety incidents will be monitored by the Governors' Curriculum, Standards and Inclusion committee and designated E-safety Governor. Please see Governing body terms of reference. Pupil conferencing sessions will be held to judge pupils' understanding of how to keep personal information safe and appropriate online behavior using the E-safety Charters.

The school will utilise the SWGfL 360 Safe self-review tool to evaluate performance, and set next steps in the computing and PSHC subject leader action plans.

Other Relevant Policies / Documents

Appendix 1 E-safety incident flow chart
Appendix 2 E-safety Charter
Appendix 3 Online Learning Platform Charter
Appendix 4 E-safety Risk Assessment

School's Acceptable Use Policy (based on SWGfL)
School's Use of Mobile Phones Policy
Governor's Terms of Reference for committees

Date: January 2022

To be revised: June 2023

Appendix 1

E-safety incident flow chart

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

↓

Record incident in behaviour book/CPOMS/Technician Log
Class teacher / Head Teacher, Designated Safeguarding Lead, 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
E-safety Leader / School Business Manager / Provider for School Website GBM (IT systems support): 07867 120 950 (Nigel Sluman), Office: 0161 605 3838 Bristol Schools IT Helpdesk: 0117 90 37999 Professional Online Safety Helpline 0344 3814771

↓

In School Action – Who is involved?			
Child Arrange meeting with Parents/Carers	**Parents/Carers** 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

E-Safety Charter

Article 13: Every child must be free to say what they think and seek all sorts of information, as long as it is within the law (not harmful to others)

- I will be responsible and behave well when using technology.
- I will always keep my passwords to myself.
- If I use websites for homework, I will try my best to make sure that they are giving me reliable information (using known sites like the BBC etc.)
- I will make sure all messages or posts sent are respectful and truthful.
- I will show a trusted adult if see something that makes me feel upset or uncomfortable.
- I will always keep my private details private (my surname, family information, phone number and address are all examples of personal information.)
- If I share photographs, I will make sure they are appropriate and not harmful or upsetting to anyone and not personal photo/photos of myself.
- I will never agree to meet someone over the Internet.
- I will never talk to strangers over the internet.

I agree to keep these rules both inside and outside of school

.