Online Safety Policy

Author/Person Responsible	Emma Ross (Computing Lead) Gemma Fricker (Headteacher)
Date of Ratification	**May 2022**
Review Group	Curriculum Committee
Ratification Group	FGB
Review Frequency	Every three years Subject to local education authority and/or national policy change.
Review Date	Summer 2025
Previous Review Amendments/Notes	
Related Policies	Acceptable Use Policy Computing Progression Map Education in a Connected World Keeping Children Safe in Education Safeguarding policy Anti-bullying policy
Equality Impact Assessment- Have any adverse impacts been identified under the Equalities Plan? (nb – if answered 'yes' please attach a Full Impact Assessment)	
Is there an impact on the Governor Handbook? (if 'yes' please inform Clerk)	
Chair of Governors signature	**A Shah R Lukes**

Rationale

Computing and internet safety by staff and children is an integral part of teaching and learning at Henleaze Infant school. Computing equipment and the internet is used as a tool across all areas of the curriculum, to enhance and stimulate children's learning. The internet in particular is used as a teaching tool and as a way of communicating and finding out about our world.

However, ensure that children and staff engage in safe practises when accessing the internet and are aware of the issues involved in its use. Managing and minimising the risks is key to ensuring safe practise.

This policy is intended to ensure shared understanding and consistency of practice across the school in relation to supporting children in developing the skills and knowledge necessary to make positive and appropriate behaviour choices which assist them and others in forming positive relationships and learning effectively.

Monitoring the effectiveness of this policy

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Local Authority IT providers monitor logs of internet activity (including sites visited)/filtering
- Surveys/questionnaires of pupil and parents/carers voice.

Roles and responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school

Governors/Governing Body - Safeguarding/Child Protection Governor

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Curriculum Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Child/Protection Safeguarding Governor (which will incorporate the role of Online Safety Governor). The role of the Online Safety Governor will include:

- regular updates from the Online Safety Lead in curriculum committee reports and meetings.
- monitoring of online safety incident logs
- reporting to relevant Governors at full governing body meetings

Headteacher and Designated Safeguarding lead

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Appendix 1: Responding to incidents of misuse". Online Safety BOOST includes an 'Incident Response Tool' that outlines the steps (and forms to complete) any staff facing an issue, disclosure or report, need to follow. More information is available at: https://boost.swgfl.org.uk/

- The Headteacherand Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable around Online Safety.
- The Designated Safeguarding Lead takes day to day responsibility for online safety issues (via CPoms)
- The Designated Safeguarding Lead and Deputy Designated Safeguarding Lead will monitor the effectiveness of this policy and any online safety concerns that are raised (via CPoms)
- The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from sharing of personal data, access to illegal/inappropriate materials, inappropriate on-line contact with adults/strangers, potential or actual incidents of grooming, online-bullying

Online Safety Curriculum Lead

- They take a leading role in establishing and reviewing the school online safety policies/documents
- They take responsibility for developing and implementing the school Online Safety curriculum. Supporting and training staff as required to follow this.
- They support with any incidents involving online safety and advise teaching methods and resources to address any concerns that arise.
- They should be aware of online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from sharing of personal data, access to illegal/inappropriate materials, inappropriate on-line contact with adults/strangers, potential or actual incidents of grooming, online-bullying
- They will take every opportunity to help parents understand issues surrounding online safety by sharing advice and information via newsletters, letters, website, social media and information about national/local online safety campaigns/literature.

ICT Support/School Business Manager

The school uses Bristol City Council ICT Support to manage the technical infrastructure of the school. The School Business Manager oversees and liaises with them to ensure:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and Designated Safeguarding Lead.
- that monitoring software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the staff acceptable use policy.
- they report any suspected misuse or problem to the Designated Safeguarding Lead for investigation.
- all digital communications with students/pupils/parents/carers should be on a professional level.
- they teach and review the school online safety rules regularly with pupils (see online safety rules, within the Education section below)
- online safety teaching is embedded in all aspects of the curriculum and other activities.
- ensure that in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Students/Pupils:

- are responsible for using the school digital technology systems in accordance with the school Online Safety rules and under the guidance of an adult. (see online safety rules, within the Education section below)

Parents/carers and Visitors to the school

- Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. They will be encouraged to support the school in promoting good online safety practice and to follow guidelines set out in our **Acceptable Use Policy.**

Education

Henleaze Infant School will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners.
Pupils will receive a broad online safety curriculum with staff reinforcing messages across all areas of the curriculum whenever technology is in use.

Our computing curriculum has been reviewed to ensure that it covers important aspects from the **'Education in a Connected World'** document from 2020.

Our Curriculum Aims
We have clear prorgressive objectives set out for each year group in our **'Computing Progression Map'**, with our main aims being that by the time pupils leave Henleaze Infants School they are able:

- To know our school Online Safety Rules and be able to explain what they mean.
- To know the importance of being kind online, just like in the real world..
- To name trusted adults that they can ask for help if they see something that they don't like online.
- To know what private information is and not to share private information online; knowing that once information is put online it is difficult to remove (digital footprint).

- To understand the importance of keeping their log in details safe and the importance of logging out when they have finished.
- To know some people can be unkind online and to ask for help, just like if someone is unkind in the real world.
- To know not to trust everything they read or see online and to check how reliable a source is.

How we deliver our Online Safety Curriculum

As well as weaving discussions about online safety throughout the curriculum pupils will have termly class sessions about online safety.

- Our termly sessions will all have a different focus and learning objectives and are planned and mapped out to build on previous knowledge to ensure progression across year groups.
- We have three sessions a year using the Common Sense Media lesson plans. This resource enables us to teach online safety using Henleaze Junior School also use this resource to support their online safety teaching so this offers progression throughout our school and beyond.
- We aim to link our online safety sessions to link in with times when we are using technology or the internet in our learning, often just before a computing session, in order to give them more meaning.
- The school participates in Safer Internet Day each year and activities are planned for each group as part of the day to fit in with the progression of our online safety curriculum. We also have Key Stage assemblies to reinforce key online safety messages.
- To support online safety teaching the school uses a range of other resources to support this, including:
    - Smartie Penguin - used to facilitate assemblies on Safer Internet Day
    - Digiduck books and other physical stories ae used to reinforce our online safety curriculum.
    - Reinforce links to the PSHE Jigsaw curriculum by linking key messages that apply both online and offline in the real world, such as 'being kind'.

School Online Safety Rules

At Henleaze Infants we have developed our own set of whole school online safety rules which have been based on the SMART rules from Childnet (https://www.childnet.com/young-people/4-11-year-olds/get-smart/) but adapted to make them more age appropriate for the infant age children in our school. We reinforce to pupils that these rules apply wherever they are using the internet, whether that be in school or elsewhere.

The rules are displayed in every class and are recapped regularly, in particular when using the internet in class to keep them fresh in pupils minds. There will also be a bi-annual KS1 mascot competition to update the look of these rules and keep their profile high (being bi-annual will ensure that all KS1 children get the opportunity to enter the competition during their time at our school).

Parents

The school will raise parents' awareness of online safety in newsletters or other communications home, and in information via our website. High profile events such as Safer Internet Day will also be used to provide information and improve awareness for parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

The school's Online Safety rules are shared with parents at least twice a year to encourage them to start discussions with pupils and reinforce these messages at home. Other information is sent to parents in response to arising concerns/issues.

Cyber-bullying

Definition
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.

Preventing and addressing cyber-bullying.
To help prevent cyber-bullying, we will highlight the importance of being kind online and ensure pupils know to report any problems online to a trusted adult.
As a school we discuss cyber-bullying and relate it to bullying as part of our Jigsaw PSHE curriculum.

Dealing with cyber-bullying instances
In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour and Anti-bullying Policies. Where illegal, inappropriate or harmful material has been spread among pupils, the school trust will use all reasonable endeavours to ensure the incident is contained. Parents will be informed and involved in supporting education. The DSL 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.

Staff Training

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

Staff will follow the guidance of the 'Education for a connected world'. And 'Keeping children safe in education' when planning our online safety curriculum.

Staff will be updated by the Computing Lead on any relevant information or changes that would further their understanding of online safety and be supported when advice or guidance is required.

The DSL and DDSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.
Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Acceptable use policy

The Acceptable Use Policy outlines in detail the appropriate use of technology in school for staff, pupils and visitors.

Monitoring of the Online Safety Policy effectiveness

This policy will be reviewed every 3 years by the Governors in the Curriculum Committee.

Any online safety concerns will be reported to the DSL (or DDSL in their absence) and logged on CPoms to ensure thorough records are maintained.

If there are any patterns or incidents the Online Safety Lead will be available to advise on additional teaching or activities that could support or address these issues, either whole class or on an individual basis.

Pupil voice is carried out each year to review pupils' knowledge and familiarity with the school online safety rules and how to stay safe online. Also this will be used to find out what games/software etc is currently being used by pupils to stay aware of potential adaptations that may be needed to the online safety curriculum in the future.

Appendix

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above). Online Safety BOOST includes a comprehensive and interactive 'Incident Management Tool' that steps staff through how to respond, forms to complete and action to take when managing reported incidents (https://boost.swgfl.org.uk/)

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.