HOLSWORTHY
C OF E PRIMARY SCHOOL
Working together, growing together, all to flourish

Holsworthy C of E Primary School

Online Safety Policy

Approved by:	TPSalvadori	Headteacher	**Date:** 28/09/2023
Approved by:	CHurley	Online safety coordinator	**Date:** 28/09/2023
Approved by:	Tracey Webster	Chair of Governors	**Date:** 28/09/2023
Last reviewed on:			
Next review due by:	28/09/2025		

Rational

Online technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe access to the internet and other communication technologies at all times.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce any risks. The Online Safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Roles and responsibilities

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. The role of the Online Safety link Governor will include:

- regular meetings with the Online Safety Coordinator
- regular monitoring of Online Safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committee / meeting

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including Online Safety) of members of the school community, though the day to day responsibility for Online Safety will be delegated to the Online Safety Coordinator (Computing Lead).
- The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Coordinator (Computing Lead) and other relevant staff receive suitable CPD to enable them to carry out their Online Safety roles and to train other colleagues, as relevant
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles..
- The Headteacher and another member of SLT 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.

Online Safety coordinator (Computing Lead)

- takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technical staff provision (2023 Westward IT)
- receives reports of Online Safety incidents from SWGfL and SENSO. SENSO to maintain a log of incidents to inform future Online Safety developments
- meets regularly with Online Safety link Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

Network Manager / Technical staff (2023 Westward IT):

ICT Technician (2023 Westward IT) is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack (anti virus software, spyware, user permission to access server, limit on PC settings)
- that the school meets the Online Safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance
- SWGfL is informed of issues relating to the filtering applied by the Grid
- 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. Disseminates information monthly, receives up to date newsletters.
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Coordinator / Officer / Headteacher / Senior Leader / Computing Co-ordinator for investigation / action / sanction
- 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 school ICT Acceptable Use Agreement
- they report any suspected misuse or problem to the Online Safety Coordinator / Officer / Headteacher
- digital communications with pupils should be on a professional level and only carried out using official school systems
- Online Safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school Online Safety and acceptable use policy. Staff are aware of any children who have not, and what this means for their usage of ICT.
- they monitor ICT activity in lessons, extra-curricular and extended school activities
- they are aware of Online Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices 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

Designated person for child protection (DSL)

should be trained in Online Safety issues and be aware of the potential for serious child protection 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
- cyber-bullying

Online Safety Committee

Members of the Online Safety committee (or other relevant group) will assist the Online Safety Coordinator (or other relevant person, as above) with:

- the production / review / monitoring of the school Online Safety policy / documents.
- the production / review / monitoring of the school filtering policy (if the school chooses to have one)

Pupils:

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Online Safety pupils

- A planned Online Safety programme should be provided as part of Computing / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- pupils should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information
- pupils should be helped to understand the need for the student / pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet will be posted in all rooms and displayed on log-on screens
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Online Safety parents

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site
- Parents evenings
- Reference to the SWGfL "Golden Rules" for parents

Monitoring

The school will monitor the impact of the policy using:

- Logs of reported incidents
- SWGfL/SENSO monitoring logs of internet activity (including sites visited)

Education & Training – Staff

It is essential that all staff receive Online Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal Online Safety training will be made available to staff.
- All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and Acceptable Use Agreement

- The Online Safety Coordinator (or other nominated person) will receive regular updates through attendance at SWGfL/LA/other information/ training sessions and by reviewing guidance documents released by BECTA/SWGfL / LA and others.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Coordinator will provide guidance / training as required to individuals as required

Training – Governors

Governors should take part in Online Safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in ICT / Online Safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / SWGfL or other relevant organisation.
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

- The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their Online Safety responsibilities
- School ICT systems will be managed in ways that ensure that the school meets the Online Safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Agreement and any relevant Local Authority Online Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems.
- All users will be provided with a group username and password
- The “master / administrator” passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe)
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by SWGfL
- The school has provided enhanced user-level filtering through the use of anti-virus filtering.
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by nominated senior leader.
- Any filtering issues should be reported immediately to SWGfL.
- Requests from staff for sites to be removed from the filtered list will be considered by Westward IT and SLT. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Committee.
- An appropriate system is in place for users to report any actual / potential Online Safety incident to the Network Manager (or other relevant person).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed procedure is in place for the provision of temporary access of “guests” (e.g. trainee teachers, visitors) onto the school system.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

Online Safety should be a focus in all areas of the curriculum and staff should reinforce Online Safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that 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.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove specific sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- pupils should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information
- pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images - Photographic, Video

- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
  pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils 'full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school
- Pupil's work can only be published with the permission of the student / pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they

- At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

This policy will be reviewed every 2 years.