Hindhayes Online Policy

eLIM School Online Safety Policy

Insert school logo

This policy sets out the ways in which the school will:

- educate all members of the school community on their rights and responsibilities with the use of technology;
- build both an infrastructure and culture of Online Safety;
- work to empower the school community to use the Internet as an essential tool for life-long learning.

This policy is used in conjunction with other school policies and has been developed by a working group, which included representatives from all groups within the school.

The Online Safety policy will be reviewed annually and will be under continuous revision in response to significant new developments in the use of technologies, new threats to Online Safety or incidents that have taken place.

The Online Safety policy approved by Governing body on: _____

Signature of Chair of Governors: _____

The next review date is: _____

Contents

Scope of policy

This policy applies to all members of the school community, including staff, pupils, volunteers, parents/carers, visitors and community users.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents such as cyber-bullying, which may take place out of school, but are linked to membership of the school.

The school will manage Online Safety as described within this policy and associated behaviour and anti-bullying policies, and will inform parents and carers of known incidents of inappropriate Online Safety behaviour that take place in and out of school.

Schedule for Development, Monitoring and Review

The Implementation of the Online Safety policy will be monitored by an Online Safety working group, meeting termly and reporting to the Governors annually.

The impact of the policy will be monitored by the Online Safety working group by looking at:

- the log of reported incidents
- the Internet monitoring log
- surveys or questionnaires of learners, staff, parents and carers
- other documents and resources
- future developments

Roles and responsibilities

The Headteacher is responsible for ensuring the safety (including Online Safety) of all members of the school community.

The Online Safety Leader who working with the designated Child Protection Coordinator will have an overview of the serious child protection issues that arise from sharing of personal data, access to illegal or inappropriate materials, inappropriate online contact with adults, potential or actual incidents of grooming and cyber-bullying.

An Online Safety working group will work with the Online Safety Leader to implement and monitor the Online Safety policy and AUPs (Acceptable User Policies). This group is made up of Online Safety Leader, Child Protection Coordinator, teacher, governor, member of support staff, technician, member of senior leadership team and pupils. School Council pupils are part of this group, working with them through the school council, to contribute their knowledge and use of technology. They meet on a termly basis.

Role	Responsibility
Governors	• Approve and review the effectiveness of the Online Safety Policy • Delegate a governor to act as Online Safety link- Janet Day • Online Safety Governor works with the Online Safety Leader to carry out regular monitoring and report to Governors
Head Teacher and Senior Leaders	• Ensure that all staff receive suitable CPD to carry out their Online Safety roles • Create a culture where staff and learners feel able to report incidents • Ensure that there is a progressive Online Safety curriculum in place • Ensure that there is a system in place for monitoring Online Safety • Follow correct procedure in the event of a serious Online Safety allegation being made against a member of staff or pupil • Inform the local authority about any serious Online Safety issues • Ensure that the school infrastructure/network is as safe and secure as possible • Ensure that policies and procedures approved within this policy are implemented • Use an audit to annually review Online Safety with the school's technical support
Online Safety Leader	• Lead the Online Safety working group • Log, manage and inform others of Online Safety incidents and how they have been resolved where this is appropriate • Lead the establishment and review of Online Safety policies and documents • Lead and monitor a progressive Online Safety curriculum for pupils • Ensure all staff are aware of the procedures outlined in policies relating to Online Safety • Provide and/or broker training and advice for staff • Attend updates and liaise with the LA Online Safety staff and technical staff • Meet with Senior Leadership Team and Online Safety Governor to regularly discuss incidents and developments • Coordinate work with the school's designated Child Protection Coordinator

Teaching and Support Staff	• Participate in any training and awareness raising sessions • Read, understand and sign the Staff AUP • Act in accordance with the Acceptable User Policies and Online Safety Policy • Report any suspected misuse or concerns to the Online Safety Leader and check this has been recorded • Provide appropriate Online Safety learning opportunities as part of a progressive Online Safety curriculum and respond • Model the safe use of technology • Monitor ICT activity in lessons, extracurricular and extended school activities • Demonstrate consistently high standards of personal and professional conduct especially in relation to use of social networks, making sure that these are in line with school ethos and policies, including at the time of a Critical Incident
Pupils	• With help read, and understand the Pupil AUP and the agreed class Internet rules • Participate in Online Safety activities, follow the AUP and report concerns for themselves or others • Understand that the Online Safety Policy covers actions out of school that are related to their membership of the school
Parents and Carers	• Endorse (by signature) the Pupil Acceptable User Policies • Discuss Online Safety issues with their child(ren) and monitor their home use of technology (including tablets, mobile phones and games devices) and the Internet • Access the school website in accordance with the relevant school Acceptable User Policies • Keep up to date with issues through newsletters and other opportunities • Inform the Headteacher of any Online Safety issues that relate to the school • Maintain responsible standards when using social media to discuss school issues
Technical Support Provider	• Ensure the school's ICT infrastructure is as secure as possible and is protected from misuse or malicious attack • Ensure users may only access the school network through an enforced password protection policy • Maintain and inform the Senior Leadership Team of issues relating to filtering • Keep up to date with Online Safety technical information and update others as relevant • Ensure use of the network is regularly monitored in order that any misuse can be reported to the Online Safety Leader for investigation • Ensure monitoring systems are implemented and updated • Ensure all security updates are applied (including anti-virus and Windows) • Sign an extension to the Staff AUP detailing their extra responsibilities
Community Users	• Sign and follow the Guest/Staff AUP before being provided with access to school systems • Use the Online Compass tool to review Online Safety

Education of pupils

Pupils to 'understand what constitutes unsafe situations and are highly aware of how to keep themselves and others safe in different situations including in relation to Online Safety'

School Inspection Handbook - Ofsted 2014

A progressive planned Online Safety education programme takes place through discrete lessons and across the curriculum, for all children in all years, and is regularly revisited.

Breadth and progression is ensured through implementation of the 2014 Somerset Byte awards and the Online Safety progression that is part of the Somerset Primary Computing Curriculum/Somerset Byte Guide to SWGfL Digital Literacy Materials.

Within this:

- key Online Safety messages are reinforced through assemblies, Safer Internet Week (February), anti-bullying week (November) and throughout all lessons
- pupils are taught to keep themselves safe online and to be responsible in their use of different technologies as detailed in the Somerset Byte scheme of work
- pupils are guided to use age appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material
- in lessons where Internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in Internet searches
- pupils are taught to be critically aware of the content they access online and are guided to validate the accuracy and reliability of information
- pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet
- pupils are taught about current issues such as online gaming, extremism, vlogging and obsessive use of technology
- parents will share the pupils AUP with them when they join the school
- pupils are educated to recognise and respond appropriately to 'different forms of bullying, including onlinebullying'

Education and information for parents and carers

Parents and carers will be informed about the ways the Internet and technology is used in school. They have a critical role to play in supporting their children with managing Online Safety risks at home, reinforcing key messages about Online Safety and regulating their home experiences. The school supports parents and carers to do this by:

- providing clear Acceptable User Policies guidance which they are asked to sign with their children and regular newsletter and website updates;
- raising awareness through activities planned by pupils;
- inviting parents to attend activities such as Online Safety week, Online Safety assemblies or other meetings as appropriate;
- providing and maintaining links to up to date information on the school website

Training of Staff and Governors

There is a planned programme of Online Safety training for all staff and governors to ensure they understand their responsibilities, as outlined in this, and the AUPs. This includes:

- an annual audit of the Online Safety training needs of **all** staff
- **all** new staff and governors receiving Online Safety training as part of their induction programme
- providing information to supply and student teachers on the school's Online Safety procedures
- the Online Safety Leader receiving regular updates through attendance at SWGfL and LA training sessions and by reviewing regular Online Safety newsletters from the LA
- this Online Safety Policy and its updates being shared and discussed in staff meetings and in Governor meetings
- the Online Safety Leader providing guidance and training as required to individuals and seeking LA support on issues
- staff and governors are made aware of the UK Safer Internet Centre helpline 0844 381 4772

Online Bullying

Online Bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

The school will follow procedures in place to support anyone in the school community affected by Online Bullying.

Pupils and staff are made aware of a range of ways of reporting concerns about Online Bullying e.g. telling a trusted adult, Online bully box, Childline Phone number 0800 1111.

Pupils, staff and parents and carers will be encouraged to report any incidents of Online Bullying and advised to keep electronic evidence.

All incidents of Online Bullying reported to the school will be recorded by the school.

The school will follow procedures to investigate incidents or allegations of Online Bullying.

The school will take steps where possible and appropriate, to identify the bully. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police.

Pupils, staff and parents and carers will be required to work with the school to support the approach to Online Bullying and the school's Online Safety ethos.

Sanctions for those involved in Online Bullying will follow those for other bullying incidents and may include:

- the bully being asked to remove any material deemed to be inappropriate or the service provider being contacted to remove content if the bully refuses or is unable to delete content
- Internet access being suspended at the school for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or AUP
- the parent and carers of pupils being informed
- the police being contacted if a criminal offence is suspected

Sexting

The school will provide appropriate support for sexting incidents which take place in and out of school. Within school, any device which has an intimate sexting image or is suspected of having such an image, will be secured and switched off. This will then be reported to the safeguarding lead. An individual member of staff will not investigate, delete or pass on the image. The safeguarding lead will record any incident of sexting and the actions taken in line with advice from Somerset Local Authority.

Prevent

The school works to ensure children are safe from terrorist and extremist material when accessing the internet on the premises. Appropriate levels of filtering are in place through a managed filtering service which includes terms related to terrorism. Children are educated to evaluate information accessed with a reporting procedure that identifies inappropriate sites so that action, including blocking can be put into place.

-

Technical Infrastructure
The person(s) responsible for the school's technical support and those with administrator access to systems will sign a technician's AUP, in addition to the staff AUP.

The school ensures, when working with our technical support provider that the following guidelines are adhered to:

- the School ICT systems are managed in ways that ensure that the school meets Online Safety technical requirements
- there are regular reviews and audits of the safety and security of school ICT systems.
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations and other devices from accidental or malicious attempts which might threaten the security of the school systems and data with regard to:
    - the downloading of executable files by users
    - the extent of personal use that users (staff/pupils/community users) and their family members are allowed on laptops and other portable devices used out of school
    - the installing programs on school devices unless permission is given by the technical support provider or Computing/ICT coordinator
    - the use of removable media (e.g. memory sticks) by users on school devices. (see School Personal Data Policy for further detail)
    - the installation of up to date virus software
- access to the school network and Internet will be controlled with regard to:
    - users having clearly defined access rights to school ICT systems through group policies
    - users (apart from possibly Foundation Stage and Key Stage One pupils) being provided with a username and password
    - staff users being made aware that they are responsible for the security of their username and password which they are required to change every 60 days; they must not allow other users to access the systems using their log on details
    - the 'master/administrator' passwords are available to the Headteacher and kept in the school safe
    - users must immediately report any suspicion or evidence that there has been a breach of security
    - an agreed process being in place for the provision of temporary access of "guests" (e.g. trainee or supply teachers, visitors) onto the school system. All "guests" must sign the staff AUP and are made aware of this Online Safety policy
    - Key Stage 1 pupils' access will be supervised with access to specific and approved online materials

- the Internet feed will be controlled with regard to:
    - the school maintaining a managed filtering service provided by an educational provider
    - the school monitoring Internet use
    - requests from staff for sites to be removed from the filtered list being approved by the Senior Leadership Team and logged using a proforma
    - requests for the allocation of extra rights to users to by-pass the school's proxy servers being recorded, agreed and logged
    - filtering issues being reported immediately
- the IT System of the school will be monitored with regard to:
    - the school IT technical support regularly monitoring and recording the activity of users on the school IT systems
    - Online Safety incidents being documented and reported immediately to the Online Safety Leader who will arrange for these to be dealt with immediately in accordance with the AUP

Data Protection

The schools Data Protection Policy provides full details of the requirements that need to be met in relation to the Data Protection Act 1998.

The school will:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- use personal data only on secure password protected computers and other devices
- ensure that users are properly 'logged-off' at the end of any session in which they are accessing personal data
- store or transfer data using approved services such as remote access, the Somerset Learning Platform (SLP), encryption and secure password protected devices
- make sure data is deleted from the device or SLP once it has been transferred or its use is complete

Use of digital and video images

Photographs and video taken within school are used to support learning experiences across the curriculum, to share learning with parents and carers on our school's learning platform and to provide information about the school on the website. The school will:

- when using digital images, instruct staff to educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites
- allow staff to take images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images
- make sure that images or videos that include pupils will be selected carefully with their knowledge
- seek permission from parents or carers before images or videos of pupils are electronically published
- Encourage pupils to seek permission from other pupils to take, use, share, publish or distribute images of them without their permission
- all parties must recognise that any published image could be reused and repurposed
- make sure that pupils' full names will not be used anywhere on the school website, particularly in association with photographs, unless permission has been given in advance
- not publish pupils' work without their permission and the permission of their parents
- keep the written consent where pupils' images are used for publicity purposes, until the image is no longer in use
- publish a policy regarding the use of photographic images of children which outlines policies and procedures including disposal and deletion

Communication (including use of Social Media)

A wide range of communications technologies have the potential to enhance learning. The school will:

with respect to email

- ensure that the school uses a secure business email system for communication
- ensure that personal information is not sent via unsecure email
- ensure that governors use a secure email system
- ensure that any digital communication between staff and pupils or parents and carers is professional in tone and content
- make users aware that email communications will be monitored by the school
- inform users what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature
- teach pupils about email safety issues through the scheme of work and implementation of the AUP
- only publish official staff email addresses where this required

with respect to mobile phones

- inform staff that personal mobile phones should only be used at break, lunchtimes and in restricted areas when they are not in contact with pupils', unless they have the permission of the Head Teacher
- inform staff that they are not allowed to use personal devices to take photographs or video in school for any purpose without the express permission of the Senior Leadership Team
- inform all that personal devices should be password protected
- advise staff not to use their personal mobile phone to contact pupils, parents and carers
- provide a mobile phone for activities that require them
- inform visitors of the school's expectations regarding the use of mobile phones

with respect to publishing work

- the contact details on the Website should be the school address, email and telephone number. Staff or pupils personal information will not be published
- written permission from parents/ carers will be obtained before photographs of pupils are published on the school website
- pupils work can only be published with the permission of the pupil and parents

with respect to social networking and personal publishing

- the school will block/ filter access to social networking sites
- newsgroups will be blocked unless a specific use is approved
- pupils will be advised never to give out personal details of any kind which may identify them or their location
- pupils and parents will be advised that they use of social network spaces outside school is not appropriate for primary aged children

with respect to other personal devices

- The staff AUP will apply to staff using their own portable device for school purposes
- enable and insist on the use of the school's Internet connection while on the school site
- maintain the right to collect and examine any device that is suspected of containing offensive, abusive or illegal content or is suspected of causing issues on the school Internet connection