



Online Safety Policy

Written by:	Computing Manager	Reviewed by:	Curriculum Committee
Review Date:	March 2025	Next Review Date:	March 2026
Review Cycle:	Annually	Ratified by CC:	12.3.25
Name: Pauline Warnants		Signature: 	

Technical staff

Those with technical responsibilities are responsible for ensuring:

- that the *school's* technical infrastructure is secure and is not open to misuse or malicious attack
- that the *school* meets required online safety technical requirements and any Hampshire online safety policy that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy

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/agreement (AUP)
- they report any suspected misuse or problem to the Headteacher for investigation/action/sanction
- all digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems
- All third-party websites must be evaluated for appropriateness and reliability prior to use, and the responsibility for the content of this data rests solely with the teacher.
- Designated Safeguarding Lead/Designated Person/Officer

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

Students/Pupils:

- are responsible for using the school digital technology systems in accordance with the student/pupil acceptable use agreement

Policy Statements

Education – Students/Pupils

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways: A planned online safety curriculum should be provided as part of Computing/PDL/other lessons and should be regularly revisited

- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Students/pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Students/pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students/pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students/pupils will be equipped with the skills to critically evaluate online issues and address them appropriately as they arise.

Education & Training – Staff/Volunteers

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:

- An audit of the online safety training needs of all staff will be carried out and these findings will help formulate a formal online safety training session which 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 agreements.

Training – Governors/Directors

Governors/Directors should take part in online safety training/awareness sessions,

Technical – infrastructure/equipment, filtering and monitoring

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password. Users are responsible for the security of their username and password
- Internet access is filtered for all users.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- *Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.)*

Mobile Technologies

- The school acceptable use agreements for staff and parents/ carers will give consideration to the use of mobile technologies

Use of digital and video images

- 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 e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website/social media/local press

Data Protection

The school must ensure that:

- it has a Data Protection Policy.
- it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- it has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
- it has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it

- the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- it will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. The school should develop and implement a 'retention policy' to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- it provides staff, parents, volunteers, teenagers and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice
- procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
- it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- it understands how to share data lawfully and safely with other relevant data controllers.
- it [reports any relevant breaches to the Information Commissioner](#) within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- If a maintained school, it must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

- data must be encrypted and password protected.
- device must be password protected.
- device must be protected by up to date virus and malware checking software
- data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Staff must ensure that:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse

- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- will not transfer any school personal data to personal devices except as in line with school policy
- access personal data sources and records 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

Communications

- The official *school* email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers must be professional in tone and content.

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.

