

**Hardenhuish School**

**ICT and Online Safety Policies and Appendices**

This policy identifies how Hardenhuish intends for the school community to remain safe through the responsible use of technology and associated resources.

**Related Policies and Procedures:**

Pupil Acceptable Use Policy (AUP)

Staff Acceptable Use Policy (AUP)

School Password Security Procedure

Cyberbullying - A Code of Conduct

Cyberbullying Protocol

Anti-Bullying Policy

Safeguarding Policy

Positive Behaviour Policy

**Background**

As part of its duty of care, Hardenhuish supports its community to use communications technology in a safe and appropriate manner. The development and implementation of this Online Safety policy involves all the stakeholders in a young person’s education from the headteacher and governors to senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of digital tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

* Access to illegal, harmful or inappropriate images or other content
* Unauthorised access to, loss of, or sharing of personal information
* The risk of being subject to grooming by those with whom they make contact on the internet
* The sharing of personal images without an individual’s consent or knowledge
* Inappropriate communication or contact with others, including strangers
* Cyberbullying
* The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks exist offline so this policy must be applied alongside the Positive Behaviour and Safeguarding policies. It is impossible to completely remove these risks, so it is essential to build pupils’ confidence and skills to mitigate these risks through educational provision.

**Development, Monitoring and Review**

This policy has been developed by the ICT Support Manager in conjunction with the Curriculum Leader for ICT.

The policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety, or incidents that have taken place. The next anticipated review date will be 12 months from approval date.

Should serious online incidents take place, external agencies including the police may be informed.

The school will monitor the impact of the policy using:

* Monitoring of reported incidents
* RM SafetyNet, Smoothwall and senso AI and human monitoring logs of internet activity (including sites visited)
* Senso and CPOMS safeguarding software

**Scope of the Policy**

This policy applies to everyone who interacts with school ICT systems including but not limited to staff, pupils, parents, governors, and volunteers.

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.

The school will deal with incidents within the scope of this policy (and associated positive behaviour and anti-bullying policies) occurring during school hours and utilising school ICT services, or where the reputation of the school or the staff are at risk. Incidents of which we become aware happening outside this remit will be reported to parents and may be reported to outside agencies where appropriate.

**Roles and Responsibilities**

**Governors:**

* Are responsible for the approval of the Online Safety policy and for reviewing its effectiveness.
* Are involved in regular meetings and monitor appropriate handling of incidents
* Take part in online safety training/awareness sessions, with particular importance for those who are members of any committee involved in ICT, Online Safety, Health and Safety, Safeguarding

**Headteacher and Senior Leaders:**

* The Headteacher is responsible for ensuring the safety of members of the school community
* Senior Leaders are responsible for ensuring that the Curriculum Leader for ICT and other relevant staff receive suitable continuous professional development to enable them to carry out their roles and to train colleagues

**Curriculum Leader for ICT:**

* Communicates with a range of external partners when reviewing online safety incidents or delivering training
* Arranges online safety training and provides advice for staff
* Liaises with ICT Support staff
* Receives reports of online safety incidents when they happen and liaises with appropriate staff to evaluate if further action is required on a whole school level (e.g. assembly)
* Takes an active role in the development and review of the ICT and PSHE curriculum

**ICT Support Manager:**

* Ensures that the school’s ICT systems are secure and protected from abuse or malicious attack
* Implements technical requirements outlined in the Acceptable Use Policy and any relevant legislation and guidance
* Protects user accounts with Multi-Factor Authentication (MFA) where relevant and applies Conditional Access policies to school resources as appropriate
* Informs RM Education of issues relating to the filtering applied at ISP level
* Regularly monitors school ICT services to identify attempted misuse and reports to the relevant staff for further action

**Staff:**

* Have an up-to-date awareness of online safety matters and of the current school Online Safety policy and practices
* Read, understand, and follow the Staff Acceptable Use Policy (AUP)
* Report any suspected misuse or problem to the Curriculum Leader for ICT
* Use only official school systems for communication with pupils and parents
* Embed online safety issues in appropriate aspects of the curriculum and other school activities
* Assist pupils to understand and follow the Online Safety and Acceptable Use policies
* Are aware of online safety issues related to the use of mobile phones, tablet devices, cameras and other devices, monitor their use, and implement school policies related to these devices

**Education and 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:

* All new staff will receive the Online Safety policy as part of their induction programme, ensuring that they fully understand the school Online Safety and Acceptable Use policies
* All staff are expected to read the Online Safety policy as part of the safeguarding documentation on an annual basis and confirm that they have done this
* The Curriculum Leader for ICT will ensure that they remain as up to date as possible regarding issues and technologies that may affect the school’s policy and appropriate response

**Designated Safeguarding Lead:**

* Takes day-to-day responsibility for online safety issues
* Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
* will be trained in online safety issues and be aware of the potential for harm to arise from:
  + sharing of personal data
  + the impact of a ‘digital footprint’
  + access to inappropriate or illegal materials
  + inappropriate online contact
  + potential or actual incidents of grooming
  + cyberbullying
  + sharing of images including sexting
  + child sexual exploitation
  + mental health and wellbeing when using digital devices

**Pupils:**

* use the school ICT systems in accordance with the Pupil Acceptable Use Policy
* understand the importance of reporting abuse, misuse or access to inappropriate materials, and know how to do this
* understand school policies on the use of mobile phones and other devices
* understand school policies on the creation and sharing of images
* understand school policies on cyberbullying

**Education – pupils**

The education of pupils in online safety is an essential part of the school’s provision. Young people need the help and support of the school to recognise and avoid risks and build their resilience.

Online Safety education will be provided in the following ways:

* A planned programme will be provided as part of ICT, PSHE, and other lessons, and will be regularly revisited, at least annually. This will cover both the use of ICT and new technologies in school and outside school.
* Key online safety messages will be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
* Staff will act as good role models in their use of ICT, the internet and mobile devices.

**Parents:**

Parents play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Research shows that many parents do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues and provide information about online safety resources*.*

**Education – parents**

Many parents have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of a young person’s online experiences. Parents often either underestimate or do not realise how often young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

The school will therefore seek to provide information and awareness to parents through methods including its website, letters, social media, and Parent Information, Advice and Guidance evenings.

**Technical – infrastructure/equipment, filtering and monitoring**

The school is responsible for ensuring that its ICT systems are as safe and secure as is reasonably possible and that 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 policy technical requirements outlined in the Acceptable Use Policy and any other relevant guidance
* There will be regular reviews and audits of the safety and security of school ICT systems
* Servers, wireless systems and cabling will be securely located and physical access restricted
* All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by a member of the ICT Support team and will be reviewed at least annually
* All users will be provided with a unique username and password
* Administrator passwords for school ICT systems are limited to ICT Support staff, recorded in an encrypted, compliant cloud-based database
* Users will be responsible for the security of their username and password, will not allow other users to use their credentials and will immediately report any suspicion or evidence that there has been a breach of security. Artificial Intelligence and “smart” rules are implemented to automatically alert ICT Support staff to activity on ICT services which requires review
* The school has a managed filtering service provided by RM Education
* The school provides enhanced user-level filtering through the use of the Smoothwall filtering software.
* Any filtering issues will be reported to the relevant service provider
* ICT Support staff will monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy
* Remote management tools are used by staff to control workstations and view users’ activity.
* An appropriate system is in place (email Helpdesk or visit ICT Office) for users to report any actual/potential online safety incident to the ICT Support team
* Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, endpoints, other devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data in line with NCSC guidance
* Removeable media (e.g. USB sticks) are not permitted with a few exceptions laid out in the Information Security policy
* The school infrastructure and individual workstations are protected by up-to-date antivirus software
* Personal data will not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured

**Curriculum**

Online safety will be a focus in all areas of the curriculum and staff will 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 are 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 must be vigilant in monitoring the content of the websites that are accessed
* From time to time pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff will request via the ICT Helpdesk that the ICT Support Manager temporarily removes those sites from the filtered list for the period of study. Any request to do so will be auditable, with clear reasons for the need

**Use of photographs and video**

When using digital images, staff will inform and educate pupils about the risks associated with the creation, use, sharing, publication and distribution of images. In particular they will recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites.

* Staff are allowed to create photographs, video and audio recordings for educational purposes, but will follow school policies concerning the sharing, distribution and publication of those images. School equipment can be provided for taking photos, videos or audio recordings for educational purposes.
* Photographs, video and audio recordings published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance and relevant legislation on the use of such images.
* Permission from parents/pupils will be obtained before photographs of pupils and their names are published by the school.

**Data Protection**

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations which states that handling of personal data must be:

* Lawful, fair and transparent
* For specified, explicit and legitimate purposes
* Adequate, relevant and limited to what is necessary
* Accurate
* Kept no longer than is necessary
* Secure

Staff will ensure that they:

* 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, ensuring that they are signed out at the end of any session in which they are using personal data
* Understand that personal data relating to pupils, parents or other staff must not be removed or copied from the school ICT services and placed on mobile devices or removable media. Staff will use the secure Remote Desktop Services to access such data when needed or access data through the school’s secure cloud platforms
* Encrypt data being sent via email which includes sensitive/personal information, with the password sent via a different method of communication
* Use the school’s cloud services to store data: files should not be saved on local storage devices including personal portable hard drives. Staff should take care to save sensitive data in areas of the cloud storage with appropriate permissions and not to create anonymous access links except where absolutely necessary
* Have permission from ICT Support (under exceptional circumstances, where other methods are not possible) for data to be transported

When permission has been given for personal data to be transported on any portable computer system, USB stick or any other removable media:

* the data must be encrypted and password protected
* the data must be securely deleted from the device once it has been transferred or its use is complete

Communications

When using communication technologies the School considers the following as good practice:

* Users need to be aware that email communications may be monitored
* Users will immediately report to a member of staff the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature, and will not respond to any such email
* Any digital communication between staff and pupils or parents will be professional in tone and content

**Unsuitable/inappropriate activities**

Users must not visit internet sites, make, post, download, upload or pass on material, remarks, proposals or comments that contain or relate to:

* + pornography (including child pornography)
  + promoting discrimination of any kind
  + promoting racial or religious hatred
  + promoting illegal acts

In addition, staff must not engage in any contact with a pupil via social networking sites or share personal contact information (mobile phone numbers, home email address, etc.) with pupils. Should staff require the personal mobile phone numbers of pupils in order to contact them on an educational trip/visit, the school mobile devices will be used. The contact details of pupils will then be erased from the mobile device as soon as the trip/visit has returned safely.

**Responding to incidents of misuse**

The Curriculum Leader for ICT and Designated Safeguarding Lead will be informed immediately of any apparent or actual misuse which appears to involve illegal activity, i.e.:

* child sexual abuse images
* adult material which potentially breaches the Obscene Publications Act
* criminally racist material
* other criminal conduct, activity or materials

The Curriculum Leader for ICT or Designated Safeguarding Lead will then instigate the School Protocol on Child Protection and Online Safety.

C:\Users\tld.HARDENHUISH.066\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\RYZW8D5N\b7553190-6ff9-49aa-9c75-0d9afd4fb1f2.tif

**Appendices**

Appendix 1: Pupil Acceptable Use Policy (AUP)

Appendix 2: Staff Acceptable Use Policy (AUP)

Appendix 3: Cyberbullying - A Code of Conduct

Appendix 4: Cyberbullying Protocol