Hardenhuish School
E-Safety Policies and Appendices

E-Safety encompasses the safe and responsible use of technology and this policy identifies how Hardenhuish intends for the school community to remain safe through the responsible use of its technology and associated resources.

Related Policies and Procedures:

Pupil / Student Acceptable Usage Policy (AUP) Appendix 2 Parent Acceptable Use Policy
School Filtering Policy
Staff Internet, Email and Computer Acceptable Usage Policy (AUP)
School Password Security Policy
Cyberbullying - A Code of Conduct
Cyberbullying Protocol

Contents

Background / Rationale
The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This School E-Safety policy will help to ensure safe and appropriate use. The development and implementation of such a strategy involves all the stakeholders in a child's education from the Headteacher and governors to senior leaders and classroom teachers, support staff, parents, members of the community and the pupils/students themselves.
The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil/student achievement.
However, the use of these new 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 / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/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 reflect situations in the off-line world and it is essential that the E-Safety is used in conjunction with other school policies (e.g, Positive Behaviour, and Child Protection Policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build pupils'/students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Development/Monitoring/Review
This E-Safety Policy has been developed by the Hardenhuish E-safety Lead in conjunction with the following members of staff:

- Senior Leader
- Network Manager
- Member of ICT Teaching Staff
- Member of PSHE Teaching Staff
- Learning Manager
- Pastoral Manager

Schedule for Development/Monitoring/Review
The implementation of this E-Safety policy will be monitored by the E-Safety Coordinator/Committee.
The E-Safety 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 E-Safety or incidents that have taken place. The next anticipated review date will be 12 months from approval date.

Should serious E-Safety incidents take place, external persons/ agencies may be informed including :
Local police or law enforcement agencies, relevant service providers.

The school will monitor the impact of the policy using:
- Monitoring of reported incidents
- RM SafetyNet monitoring logs of internet activity (including sites visited)
- Senso.Cloud and MyConcern Safeguarding software
- Internal monitoring data for network activity

Scope of the Policy

This policy applies to all members of the School community (including staff, pupils/students, parents, visitors, community users) who use school equipment and systems.

The Education and Inspections Act 2006 empowers headteachers to such extent as is reasonable, to regulate the behaviour of pupils/students 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 behaviour and anti-bullying policies) occurring during school hours and utilising school technology, 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:

- Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the Policy.
- Involved in regular meetings and monitoring / appropriate handling of incidents
- **Training – Governors**
- Governors will take part in E-Safety training/awareness sessions, with particular importance for those who are members of any committee involved in ICT/E-Safety/health and safety/child protection.

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including E-Safety) of members of the school community, though the day to day responsibility for E-Safety will be delegated to the E-Safety Coordinator.
- The Headteacher/Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable continuous professional development to enable them to carry out their E-Safety roles and to train other colleagues, as relevant.
- The Headteacher and another member of the Senior Leadership Team will take the appropriate action in the event of a serious E-Safety allegation being made against a member of staff. (Hardenhuish HR/disciplinary procedures).

E-Safety Coordinator:

- Speaks and communicates with a range of qualified staff when reviewing E-safety situations or training
- takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the school E-Safety policies/documents;
- ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place;
- provides training and advice for staff;
- liaises with school ICT technical staff;
- receives reports of E-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 on issue);
- reports regularly (at least monthly) to a member of the Senior Leadership Team.
- Takes an active role in the development and reviewing of the ICT and PSHE E-safety curriculum

ICT Support Manager:

The ICT Support Manager is responsible for ensuring:

- that the school's ICT infrastructure is secure and is protected from abuse or malicious attack.
- that the school meets the E-Safety technical requirements outlined in the Acceptable Usage Policy and any relevant E Safety legislation and guidance.

- that user accounts are protected with Multi-Factor Authentication (MFA) where relevant and Conditional Access policies are applied to school resources as appropriate.
- RM Education is informed of issues relating to the filtering applied by at ISP level.
- that the use of the School's IT services are monitored regularly (at least weekly) in order that any misuse/attempted misuse can be reported to the E-Safety Coordinator 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 E-Safety matters and of the current school E-Safety Policy and practices.
- they have read, understood and signed the school Staff Acceptable Use Policy (AUP).
- they report any suspected misuse or problem to the E-Safety Coordinator for investigation/action/sanction.
- digital communications with pupils/students are on a professional level and only carried out using official School systems . School VoIP systems should not be used to communicate 1:1 between a Staff member and a pupil or student.
- E-Safety issues are embedded in all aspects of the curriculum and other school activities.
- pupils/students understand and follow the school E-Safety and Acceptable Use Policy.
- they are aware of E-Safety issues related to the use of mobile phones, , tablet devices (e.g. IPads), cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.

Education & Training – Staff
It is essential that all staff receive E-Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff will receive the E-Safety policy as part of their induction programme, ensuring that they fully understand the school E-Safety and Acceptable Use Policies.
- All staff are expected to read the E-Safety Policy as part of the safeguarding documentation on an annual basis and sign a slip to confirm that they have done this.
- The E-Safety Coordinator (or other nominated person) will ensure that they remain as up to date as possible regarding issues and technologies that may affect the school's E-safety policy and appropriate response.

Designated person(s) for Child Protection:
will be trained in E-Safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data;
- the impact of a 'digital footprint' and how this can be protected/reduced
- access to illegal/inappropriate materials;
- inappropriate on-line contact with adults/strangers;
- potential or actual incidents of grooming;
- cyberbullying.
- Sharing of images (including sexting)
- Child sexual exploitation
- Mental health and wellbeing when using digital devices

E-Safety Committee:
Members of the E-Safety committee will assist the E-Safety Coordinator with:

- the production/review/monitoring of the school E-Safety policy.
- Planning of Procedures and responses to E-Safety incidents.

Pupils/students:
are responsible for:

- using the school ICT systems in accordance with the Pupil/Student Acceptable Use Policy, which they will sign before being given access to School systems;
- understanding 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, tablet devices, and handheld devices. They will also know and understand school policies on the taking/use of images and on cyberbullying.
- will understand the importance of adopting good E-Safety practice at all times and remain compliant with the expectations identified in the AUP. .

Education – pupils/students
The education of students/pupils in E-Safety is therefore an essential part of the School's E-Safety provision. Children and young people need the help and support of the School to recognise and avoid E-Safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned E-Safety programme will be provided as part of ICT/PSHE/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 E-Safety messages will be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities, including the potential impact on mental health and strategies on how to maintain positive emotional wellbeing (for example, encouraging '5-a-day for your mental health' which includes building time into each day to 'connect' with friends/family face-to-face without technology).
- Signposting support if pupils/students need to seek further advice/guidance regarding E-safety or support for their online wellbeing.
- 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/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 through website/VLE and information about national/local E-Safety campaigns/literature*.*

Parents will be responsible for:

- endorsing (by signature) the Pupil/Student Acceptable Use Policy;

Education – parents
Many parents have only a limited understanding of E-Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents through methods including: Letters, newsletters, website, School related Twitter feeds and Parent Forums.

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 E-Safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the E-Safety technical requirements outlined in the Acceptable Usage Policy and any other relevant E-Safety 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 the Network Manager (or member of the ICT technical 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 Senior ICT Support staff, recorded in an encrypted cloud-based database managed by a reputable, experienced organisation.
- Users will be made responsible for the security of their username and password, will not allow other users to access the systems using their log on details 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 suspicious activity on Cloud services.
- The School maintains and supports the managed filtering service provided by RM Education.
- The School has provided enhanced user-level filtering through the use of the Smoothwall filtering programme.
- Any filtering issues will be reported immediately to RM Education.
- School ICT technical 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 Support Office) for users to report any actual/potential E-Safety incident to the ICT Support Manager.
- 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 policy is in place (Acceptable Use Policy - Pupil/Staff) regarding the downloading/installation of executable files by users.
- An agreed policy is in place (Staff AUP) to prevent staff from installing programmes on school workstations/portable devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school workstations/portable devices. (see School Data Protection Policy).
- The school infrastructure and individual workstations are protected by up to date anti-virus software.
- Personal data will not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

E-Safety will be a focus in all areas of the curriculum and staff will reinforce E-Safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that students/pupils will 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 students/pupils are allowed to freely search the internet (e.g. using search engines) staff be vigilant in monitoring the content of the websites that are accessed.
- It is accepted that from time to time, for good educational reasons, students 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 that the Network Manager temporarily remove 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 digital and video images - photographic and video
When using digital images, staff will inform and educate pupils/students about the risks associated with the taking, 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 take digital/video images to support educational aims, but will follow school policies concerning the sharing, distribution and publication of those images. School equipment can be provided for taking photos, videos or sound recordings linked to an educational intention.
- Photographs/videos published on the website, or elsewhere that include pupils/students will be selected carefully and will comply with good practice guidance on the use of such images.
- Permission from parents/pupils will be obtained before photographs of pupils/students and their names are published on the school website (Permission requested on the Data Collection Sheet and in line with the GDPR legislation).

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

- Lawful, fair and transparent;
- Obtained 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 properly “logged-off” at the end of any session in which they are using personal data.
- Understand that personal data relating to students, parents/carers or other staff must not be removed or copied from the school network and placed on Mobile Devices or removable media. You will use the secure Remote Desktop Services to access such data when needed or access data through the Office 365 secure platform.
- Data that must be transferred to removable media needs to be placed on encrypted removable media to ensure data integrity
- Data being sent via email which includes sensitive/personal data should be encrypted and attached, with the password sent in an additional email
- Data must be stored using enterprise Cloud services; files should not be saved on hard drives 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 device must be password protected (many memory sticks, cards and other mobile devices cannot be password protected).
- the device must be checked by approved anti-virus and malware software.
- 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:

- The official school email service may be regarded as safe and secure and is monitored.

- Users need to be aware that email communications may be monitored.
- Users will immediately report, to the E-Safety Coordinator – in accordance with the school policy, 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/students or parents (email, show my homework, Office 365, etc.) will be professional in tone and content.

Unsuitable/inappropriate activities
The School believes that the activities referred to in the following section are inappropriate in a school context and that users, as defined below, will not engage in these activities in school or outside school when using school equipment or systems.

Users will under no circumstances:

- 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
- Use the internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could be considered inappropriate.

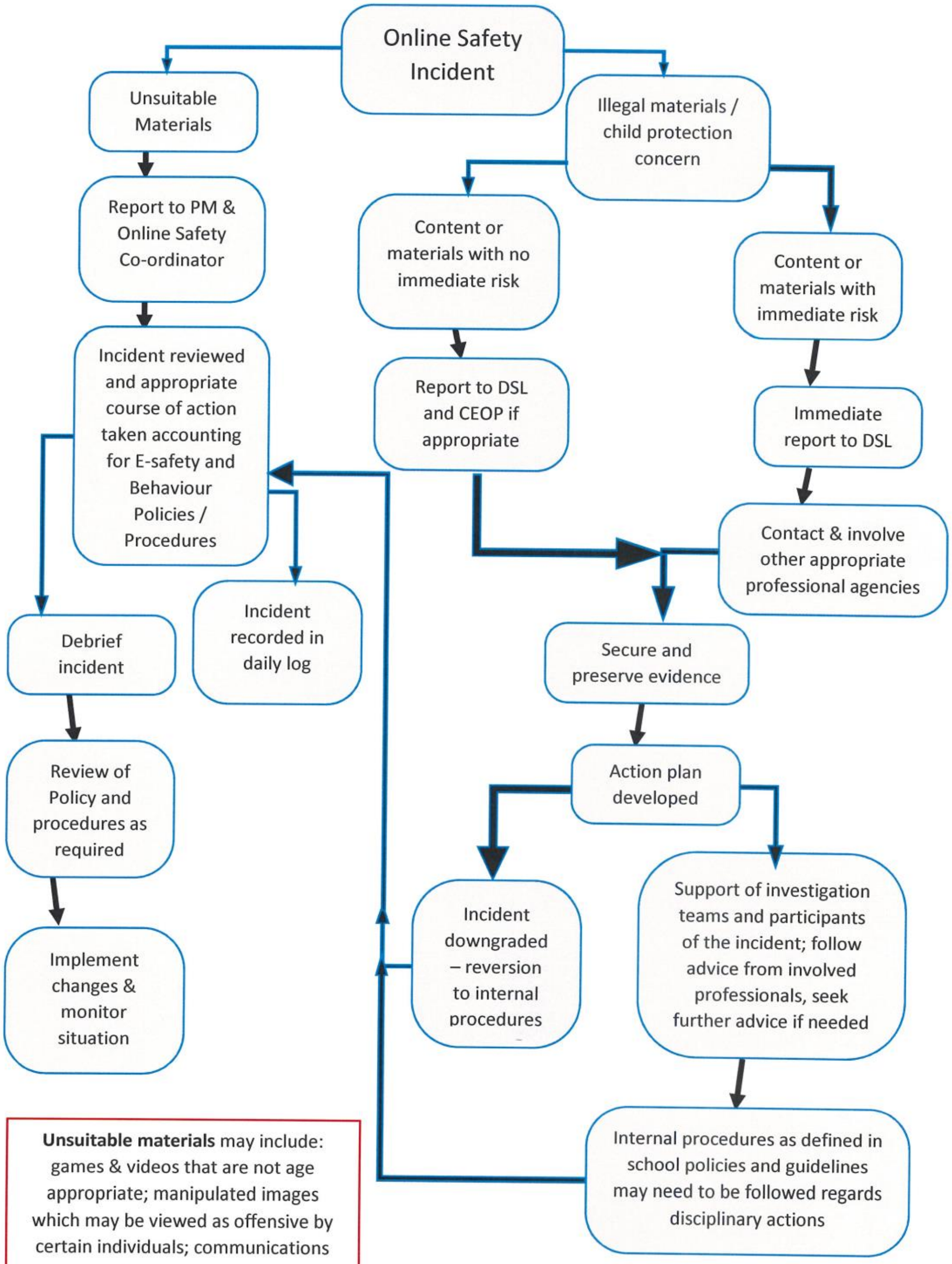
In addition, staff will not:

- engage in any contact with a pupil via social networking sites which are not approved for use by the School Senior Leadership team, 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 telephones will be used wherever possible. In any event, 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 E Safety Coordinator 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 E-Safety Coordinator or Designated Safeguarding Lead will then instigate the School Protocol on Child Protection and E-Safety.


Online Safety Incident
Unsuitable Materials
Illegal materials / child protection concern
Report to PM & Online Safety Co-ordinator
Content or materials with no immediate risk
Content or materials with immediate risk
Incident reviewed and appropriate course of action taken accounting for E-safety and Behaviour Policies / Procedures
Report to DSL and CEOP if appropriate
Immediate report to DSL
Contact & involve other appropriate professional agencies
Debrief incident
Incident recorded in daily log
Secure and preserve evidence
Review of Policy and procedures as required
Action plan developed
Implement changes & monitor situation
Incident downgraded – reversion to internal procedures
Support of investigation teams and participants of the incident; follow advice from involved professionals, seek further advice if needed
Internal procedures as defined in school policies and guidelines may need to be followed regards disciplinary actions

Unsuitable materials may include: games & videos that are not age appropriate; manipulated images which may be viewed as offensive by certain individuals; communications made in the process of bullying. These are examples only, if **in doubt – Report** concern to DSL

DSL – Designated Safeguarding Lead

Acknowledgements

Hardenhuish School acknowledges the advice and guidance received from SWGfL in the development of this School E-Safety Policy.

Appendices

Appendix 1: Pupil/Student Acceptable Usage Policy (AUP)
Appendix 2: Parent Acceptable Use Policy
Appendix 3: School Filtering Policy
Appendix 4: Staff AUP
Appendix 5 School Password Security Policy
Appendix 6 Cyberbullying - A Code of Conduct
Appendix 7 Cyberbullying Protocol