HAZLEGROVE

Deo Juvante

ICT AND E-SAFETY POLICY

E-SAFETY ADMINISTRATION

Future monitoring and development will be done by the ICT Committee. Overall responsibility for the safety and welfare of the pupils online will be taken by the Deputy Safeguarding Lead responsible for e-Safety.

e-SAFETY risks for those who have access to the School ICT system

The use of exciting and innovative ICT tools in school and at home has been shown to raise educational standards and promote pupil 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, the loss of or the sharing of personal information. The risk of grooming by those with whom they make contact on the internet.
- The sharing or distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication or contact with others, including strangers.
- Cyber-bullying
- Access to unsuitable video or internet games.
- An inability to evaluate the quality, accuracy, appropriateness and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use may impact on the social and emotional development and on the learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-Safety policy is used in conjunction with other school policies (e.g. behaviour, anti-harassment 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' resilience to online risks and minimise exposure, so that they have the confidence and skills to face and deal with these risks.

MONITORING

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Internal monitoring data for network activity
- Surveys or questionnaires of pupils through tutor time and IT lesson discussion
- Parents and Guardians
- Staff

SCOPE OF POLICY

This policy applies to all members of the school community (including staff, pupils, volunteers, parents and guardians, visitors) who have access to and are users of school ICT systems. The Education and Inspections Act 2006 empowers Heads, to such an 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 of cyber-bullying or other e-Safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

ROLES AND RESPONSIBILITIES

The following section outlines the roles and responsibilities for e-Safety of individuals and groups within the school:

HEAD

- The Head 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 DSL.

- The Head and Deputy Head are responsible for ensuring the DSL and other relevant staff receive suitable CPD to enable them to carry out their e-Safety roles and to train other colleagues, as relevant.

- The Senior Leadership Team will receive regular monitoring reports from the DSL.

- The Head and Deputy Head should be aware of the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff.

The DDSL

The Foundation Designated Safeguarding Lead is responsible for online or eSafety in the school, with regard for both pupils and staff. The Deputy Designated Lead – Child Exploitation assists the Foundation Designated Safeguarding Lead in:

- Liaising with the ICT Manager, Director of Information Systems, other key staff, and eSafety Governor as required, to promote safe use of the internet and social media by pupils.

- Responsibility for an ongoing online safety self-review.

- Completion of relevant sections of annual LSCP Safeguarding Audit and annual Safeguarding Report to Governors, if required.

- Taking day to day responsibility for e-Safety issues and has a leading role in establishing and reviewing the school e-Safety policies and documents.

- Meeting regularly with the Head to discuss current issues, review incident logs.

- Reporting regularly to Senior Leadership Team.

- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place.

- Providing training and advice for staff.

- Liaising with school ICT technical staff to ensure that the school's ICT infrastructure is secure and is not open to misuse or malicious attack.

- Receiving reports of e-Safety incidents and creates a log of incidents to inform future e-Safety developments.

- Ensuring that the school meets the e-Safety technical requirements.

- Ensuring that users may only access the school's networks through a properly enforced password protection policy.

- Ensuring that they keep themselves up to date with e-Safety technical information in order to effectively carry out their e-Safety role and to inform and update others as relevant.

- Ensuring that the use of the network including remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Head.

- Ensuring that monitoring software and systems are implemented and updated as agreed in school policies.

- Receiving training in e-Safety issues and be aware of the potential for serious child protection issues which may arise from sharing of personal data, access to illegal or inappropriate materials or inappropriate on-line contact with adults or strangers, potential or actual incidents of grooming, cyber-bullying.

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 ICT Staff Code of Conduct.
- They report any suspected misuse or problem to the DSL.
- Digital communications with pupils are on a professional level only.
- e-Safety issues are embedded in all aspects of the curriculum and other school activities.
- Pupils understand and follow the school e-Safety and Student acceptable use policies.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons, extra-curricular and extended school activities.
- They are aware of e-Safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school policies with regard to these devices.

ICT COMMITTEE

Members of the ICT committee will assist the DDSL with reviewing and monitoring the school e-Safety policy and documents.

PUPILS

- Are responsible for using the school ICT systems in accordance with the Acceptable Use Policy, which they will be expected to be familiar with.
- 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 guidance on the use of mobile phones, digital cameras and handheld devices. They should also know and understand

school policies on the taking and use of images and on cyber-bullying.

- Should understand the importance of adopting good e-Safety practice when using digital technologies out of school and realise that the school's e-Safety Policy covers their actions out of school, if related to their membership of the school.

PARENTS AND GUARDIANS

Parents and Guardians play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will therefore take the opportunity to help parents understand these issues through parents' evenings, parent forums, letters, and other literature. Parents and guardians will be responsible for endorsing (by signature) the Pupil Acceptable Use Policy.

e-SAFETY EDUCATION

PUPILS

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

- A planned e-Safety programme is provided at the beginning of each academic year for all pupils. 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 training.

- Pupils should be taught in lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.

- Pupils should be helped to understand the need for the 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.

STAFF

Staff should act as good role models in their use of ICT, the internet, and mobile devices.

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:

- Formal e-Safety training will be made available to staff.

- All new staff should receive e-Safety training as part of their induction programme,

ensuring that they fully understand the school e-Safety policy and Acceptable Use Policies.

- The DSL and ICT teachers and support staff will receive regular updates through attendance at training sessions and by reviewing any guidance documents released.
- This e-Safety policy and its updates will be presented to and discussed by staff in staff INSET days.
- The DSL and ICT teachers and support staff will provide advice, guidance and training to individuals as required.

TECHNICAL INFRASTRUCTURE

The school will be responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- 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 username and password by the ICT department who will keep an up-to-date record of users and their usernames.
- The "master administrator" passwords for the school ICT system, used by the ICT Manager must also be available to the Head or Bursar and kept in the 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 a managed filtering service.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Users should report any actual or potential e-Safety incident to the DSL.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system where they are given their own log on and restricted access.
- The school infrastructure and individual workstations are protected by up-to-date

virus software.

- Personal data should not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

CURRRICULUM

e-Safety should be a focus in all areas of the curriculum and staff should 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 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, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT Manager can temporarily remove those 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 and content they access on-line 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

- When using digital images, staff should inform and educate 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.

- Staff are allowed to take digital or video images to support educational aims, but must follow school policies concerning the sharing, distribution, and publication of those images.

- Care should be taken when taking digital or 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.

- Photographs of pupils used in the School magazines, other School publications, the School website and other promotional literature will only be used in accordance with the Parent School Contract.

DATA PROTECTION

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

The appointed Data Protection Controller for Hazlegrove is the Estates Bursar.

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 must immediately report to a suitable person – the receipt of any email that makes them feel uncomfortable, is offensive or threatening in nature and must not respond to any such email.

- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

RESPONDING TO INCIDENTS OF MISUSE

Listed below are the responses that may be made to any apparent or actual incidents of misuse. Where more than one possible sanction is listed the response will be determined by the nature and severity of the incident.

If any apparent or actual misuse 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 Head should be informed immediately and all actions taken to preserve the evidence.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence, and protect those carrying out the investigation.

It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through behaviour and disciplinary procedures.

FILTERING

The school will maintain a "best effort" filtering policy to restrict students' access to inappropriate sections of the internet. The school expects all users to use the internet responsibly and will make a "best effort" to prevent students visiting internet sites that contain or relate to:

- Pornography (including child pornography)
- Promoting discrimination of any kind
- Promoting racial or religious hatred
- Promoting illegal acts
- Any information that may be offensive to other pupils or staff.

Students' access will be monitored, and any apparently inappropriate sites will be blocked. The use of proxy sites to bypass the school filter will also be monitored and these will also be blocked.

Staff

Staff are allowed unfiltered access to the internet, but their use is logged and archived. If necessary, this can be audited, but only at the request of the Head or Bursar.

Staff may request blocked sites to be made available to students if they contain information relevant to their subjects. These sites should be blocked again when no longer required for research. Requests should be made to the ICT Manager.

APPENDIX A

UNSUITABLE AND INAPPROPRIATE ACTIVITIES

The school believes that the activities referred to in the following section would be unacceptable in a school context and that users should not engage in these activities in school or when using school equipment or systems.

User Actions

		Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images		√
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation		√
	adult material that potentially breaches the Obscene Publications Act in the UK		√
	criminally racist material in UK		√
	pornography	√	
	promotion of any kind of discrimination	√	
	promotion of racial or religious hatred	√	
	threatening behaviour, including promotion of physical violence or mental harm	√	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute	√	
Using school systems to run a private business		√	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school		√	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions		√	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)		√	
Creating or propagating computer viruses or other harmful files		√	

Actions and sanctions for incidents involving pupils misuse of the school system. The response would dependontheseverityandfrequencyoftheincident.

Incidents:	Warning	Refer to technical support staff for action re filtering / security etc	Refer to Housemaster/Tutor	Removal of network / internet access rights	Refer to Head	Inform parents or Guardians	Further sanction eg detention or exclusion	Refer to Police
Deliberately accessing or trying to access material that could be considered illegal (see list in Appendix A on unsuitable and inappropriate activities).					√	√	√	√
Unauthorised use of non-educational sites during lessons	√	√	√					
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	√	√	√					
Unauthorised use of social networking, instant messaging, personal email	√	√	√					
Unauthorised downloading or uploading of files		√	√	√				
Allowing others to access school network by sharing username and passwords			√	√				
Attempting to access or accessing the school network, using another pupil's account			√	√				
Attempting to access or accessing the school network, using the account of a member of staff			√	√	√	√		
Corrupting or destroying the data of other users				√	√	√		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature			√	√	√	√		
Continued infringements of the above, following previous warnings or sanctions							√	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school					√	√	√	
Using proxy sites or other means to subvert the school's filtering system			√	√	√	√	√	
Accidentally accessing offensive or pornographic material and failing to report the incident			√	√	√	√	√	
Deliberately accessing or trying to access offensive or pornographic material					√	√	√	
Deliberately attempting to access protected areas of the network (Hacking)					√	√	√	