Perrott Hill
E-Safety Policy

The Board of Directors has charged the Proprietor with day-to-day responsibility for the governance of the School. Ultimate responsibility for the governance of the School rests individually and collectively with Board of Directors.

The Proprietor chairs a Board of Governors acting in an advisory capacity in support of good governance.

This policy is written to include the Early Years Foundation Stage and the boarding community.

Section 1: Development, Monitoring and Review of this Policy

This e-safety policy has been developed by:

- The Head of ICT (E-Safety Co-ordinator).
- The Designated Safeguarding Lead.

Wider consultation with the whole school community has taken place through the following:

- Staff meetings and E-safety InSET.
- The Pupil ICT Committee.

Schedule for Development, Monitoring and Review

This e-safety policy was approved by the Headmaster, (Designated Safeguarding Lead), Assistant Safeguarding Lead, the Head of ICT & Computing, the Information Systems and Development Manager and the E-safety Governor:	*September 2016*
The implementation of this e-safety policy will be monitored by the:	*Head of ICT and the Designated Safeguarding Lead*
The E-safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*January 2017 and then annually*

Should serious e-safety incidents take place, the following should be informed:	*The Police.* *Designated Safeguarding Lead* *Parents or Guardians of pupil*

Section 2: E-safety risks

The use of exciting and innovative ICT tools in school and at home has the potential 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, but are not limited to:

- **CONTENT**: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **CONTACT**: being subjected to harmful online interaction with other users; for example: peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **CONDUCT**: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and seminudes and/or pornography, sharing other explicit images and online bullying.
- **COMMERCE**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Many of these risks reflect some of those in the off-line world and it is essential that this e-safety policy is used in conjunction with other School policies, for example behaviour, the counter-bullying and safeguarding & child protection policies.

As with all other risks, it is impossible to eliminate E-safety risks completely. It is therefore essential, through good educational provision, to build pupils' 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.

Section 3: Monitoring

The School will monitor the impact of the policy using:

- Logs of reported incidents on MyConcern and through regular minuted safeguarding meetings.
- Internal network activity monitoring on student devices using keystroke monitoring.
- Surveys and questionnaires of pupils, parents or guardians and staff.

Section 4: Scope of the Policy

This policy applies to all members of the School community (including staff, pupils, volunteers, parents, visitors and community users) who have access to and are users of school ICT systems, both in and out of school.

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 of cyber-bullying or other e-safety incidents, covered by this policy, which may take place out of school, e.g. behaviour linked to online gaming, but are linked to membership of the School.

The School will deal with such incidents with reference to this policy and associated behaviour and counter-bullying policies and will, where it is known, inform parents of incidents of inappropriate E-safety behaviour that take place out of school.

Section 5: Roles and Responsibilities

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

<u>Headmaster</u>

- The Headmaster 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 Co-ordinator and the Designated Safeguarding Lead.
- The Headmaster is responsible for ensuring that the E-Safety Co-ordinator 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 Headmaster and the Bursar 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.

Head of ICT and E-Safety Coordinator

- Liaises with the Designated Safeguarding Lead and the Deputy Designated Safeguarding Lead as appropriate.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Leads the Pupil Computing Committee.
- Takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the School e-safety policies and documents.
- Provides training and advice for staff and parents.
- Liaises with contractors to ensure that the School's ICT infrastructure is secure and is not open to misuse or malicious attack.
- Meets regularly with the DSL to discuss current issues, review incident logs etc.
- Keeps up to date with e-safety technical information in order to effectively carry out the e-safety role and to inform and update others as relevant.
- review the effectiveness of how E-safety is taught and all documentation.

And in conjunction with contractors:

- Works to ensure that the School's ICT network is secure and is not open to misuse or malicious attack.
- Ensures that users may only access the School's networks through a properly enforced password protection policy.
- Ensures that the School meets the e-safety technical requirements.
- Keeps up-to-date with e-safety technical information in order to work effectively alongside the E-Safety Coordinator
- Ensures 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 Headmaster.
- Ensures that monitoring software and systems are implemented and updated as agreed in School policies.

Teaching and Support Staff

Are responsible for ensuring that:

- they attend any e-safety training as requested by the Headmaster /Director of Studies. Suitable online safety training is a requirement of staff included in Keeping Children Safe in Education (2024)
- they have read and understood the policies associated with e-safety and the current Staff Acceptable Use Policy (AUP).
- they report any suspected misuse or problem to the E-Safety Coordinator or the Headmaster.
- digital communications with pupils are on a professional level and informed by the detail and spirit of the Staff Code.
- E-safety issues are embedded in any aspects of the curriculum that are appropriate and in their charge, and in other school activities as appropriate.
- pupils in their charge understand and follow the School E-safety Policy and Pupil Acceptable Use policy (Pupil AUP).
- they promote among pupils a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulation.
- 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 hand held devices and that they monitor their use and implement current school policies with regard to these devices.
- wherever possible internet use within lessons is pre-planned and pupils are guided to sites checked as suitable for their use and that the member of staff is aware of how to deal with any unsuitable material that is found in internet searches. [See also Section 8 below.]
- Liaise with the Headmaster and Head of ICT regarding what technology can be taken on school trips.

<u>Designated Safeguarding Lead and Deputy Designated Safeguarding Lead</u>

- In combination, will have training in E-safety issues and are aware of the potential for serious safeguarding issues to arise from:

  - ✓ Sharing of personal data.
  - ✓ Access to illegal or inappropriate materials.
  - ✓ Inappropriate on-line contact with adults or strangers.
  - ✓ Potential or actual incidents of grooming.
  - ✓ Cyber-bullying.
  - ✓ Extremism and radicalisation

- Liaise with the E-Safety Co-ordinator to establish, develop and review the E-safety policies, documents and curriculum.
- Attend relevant meetings.

<u>The Pupil Computing Committee</u>

The Pupil Computing Committee comprises a representative from each year from Years 3 to 8 and will assist the E-Safety Co-ordinator with ensuring that policies and practice are fit for purpose. The committee will meet regularly throughout the year.

Pupils

- are responsible for using the School ICT systems in accordance with the Pupil Acceptable Use Policy. They have to acknowledge understanding of this policy each time they log in to the School network and the policy is displayed prominently in the ICT room and in the boarders' Quiet Room.
- Should aim to develop good understanding of research skills including artificial intelligence 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 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 and Pupil AUP cover their actions out of School, if related to their membership of the School.

Parents/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 every opportunity to help parents understand these issues through a parent focus e-safety lecture (at least once every two years ideally), parents' evenings, letters and other literature. Parents are advised of the Pupil AUP and can access them at any time via the website.

Section 6: E-safety education

i. Pupils

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

- A planned e-safety programme is provided as part of the ICT and PSHE curriculum and is regularly revisited – this will cover both the use of ICT and new technologies in School and outside School.
- Key E-safety messages are reinforced as part of a planned programme of training, including the promotion of digital citizenship.
- Pupils are 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 Pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and devices both within and outside School.
- Pupils should be taught to acknowledge the source of information used and respect copyright when using material accessed on the internet.

ii. Staff

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

- It is essential that all staff, academic and support, 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 given to staff.
  - An audit of the e-safety training needs of all staff will be carried out.
  - 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 AUPs.

- The E-Safety Co-ordinator will receive regular updates through attendance at training sessions and by reviewing any guidance documents.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings or during InSET days.
- The E-Safety Co-ordinator will provide advice, guidance or training to individuals as required.

Section 7: 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.

- School ICT systems will be managed and there will be regular reviews and audits of the safety and security of the ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to the school ICT systems.
- All users will be provided with a username and password and group passwords will be used for EYFS, Year 1, and Year 2.
- The School will keep an up-to-date record of users and their usernames. Users will be required to change their password in accordance with the password protocol.
- The "administrator" password for the School ICT system must also be available to the Headmaster or Bursar.
- Users will be made responsible for the security of their username and password and must not allow other users to access the systems using their log on details. Any suspicion or evidence that there has been a breach of security must immediately be reported to the Head of ICT or the Headmaster.
- The School maintains a managed filtering service.
- The School ICT staff regularly monitor and record the activity of users on the School ICT systems and users are made aware of this in the AUPs.
- Users should report any actual or potential e-safety incident to the E-Safety Coordinator or the Designated Safeguard Lead.
- Procedure is in place for the provision of temporary access of "guests" (for example trainee teachers or visitors) onto the School system and they will sign a Staff AUP.
- The school infrastructure and individual workstations are protected by up to date antivirus software.
- Personal data cannot be sent over the internet or taken off the School site unless safely encrypted or otherwise secured.

Section 8: The Curriculum

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. It is worth staff knowing that YouTube

links can be inputted at SafeShare.tv to strip them of advertising and other unpredictable material.

- Where pupils are allowed to freely search the internet, for example when using search engines, staff should be vigilant in monitoring the content of the websites that are visited.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs or discrimination) that would normally result in internet searches being blocked. In such a situation, staff may request that the Head of ICT temporarily removes 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, and logged.
- Those points in section 6 part i. above that are relevant to the curriculum should be noted.
- Pupils are aware of the impact of cyber-bullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies, for example a parent, teacher or a trusted staff member, or an organisation such as Child Line; these are listed in the school's Circle of Care, as is CEOP in the case of a pupil having concerns about the online behaviour of another user.

Section 9: 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 communications may be monitored
- users must immediately report, to a suitable person, the receipt of any communication that makes them feel uncomfortable or that is offensive or threatening in nature and must not respond to any such communication.
- pupils should be taught about communication safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to write communications 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.

Section 10: 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 and video images to support educational and marketing aims, but must follow School policies concerning the taking, sharing, distribution and publication of those images. Further guidance on this can be found in the Staff AUP.
- A statement on the taking of digital images or video by parents or other family adults is included in section 1.5 of the Safeguarding and Child Protection Policy. This includes guidelines on the storage and use of such images. This statement is reproduced on event programmes and other such pertinent literature.
- As stated in the Staff AUP and Safeguarding & Child Protection Policy, staff working with children in the EYFS must not use personal recording equipment at any time.
- 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 other pupils or of staff without their permission.
- Photographs published on the website, or elsewhere, that include pupils will be selected carefully and will comply with the good practice guidance on the use of such images.
- Photographs of pupils used in School magazines, other School publications, the School website and other promotional literature will only be used in accordance with the parent/school contract.

Section 11: Data Protection

The School takes seriously its responsibility to ensure that data is not mishandled, stolen or misused.

GDPR / data protection, data retention and privacy are covered in their own respective policies.

Section 12: Filtering

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

- Pornography
- Child abuse
- Promoting discrimination of any kind
- Promoting racial or religious hatred
- Extremism and radicalisation
- Promoting illegal acts
- Any information that may be offensive to other pupils or staff

Pupils' 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 are allowed filtered internet access at a higher level but also their use is logged and archived. If necessary, this can be audited at the request of the Headmaster or Bursar.

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

Section 13: Responding to instances of misuse

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 DSL and/or Headmaster 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.

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.

The School believes that the activities referred to 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.

Perrott Hill
E-Safety Policy

		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	√	
Users shall not:			
Use the 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		√	
Upload, download or transmit commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions		√	
Reveal or publicise confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)		√	
Create or propagate computer viruses or other harmful files		√	

Perrott Hill
E-Safety Policy

Actions and sanctions for incidents involving pupils' misuse of the School system. The response would depend on the severity and frequency of the misuse.

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 Headmaster	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 on previous page)					√	√	√	√
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)					√	√	√	