PERRAN-AR-WORTHAL CP SCHOOL
Every Moment Matters

E-SAFETY POLICY

Background and rationale

1. Information technology (IT) is integral to the lives of children and young people in today's society, both within schools and in their lives outside school. It is a powerful tool, which opens up new opportunities for everyone, helps teachers and pupils learn from each other, stimulates discussion, promotes creativity and promotes effective learning.

2. However, children and young people should have an entitlement to safety at all times. The requirement to ensure that children are able to use IT appropriately and safely is addressed as part of the wider duty of care, to which all who work in schools are bound. This e-safety policy aims to ensure safe and appropriate use.

Possible dangers

3. The use of new technology has been shown to raise educational standards and promote pupil achievement. However, this can put young people at risk within and without the school. Some of the dangers include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to, loss of or sharing of personal information
- Grooming by those with whom they make contact on the internet
- Sharing or distributing personal images without an individual's consent or knowledge
- Inappropriate communication or contact with others, including strangers
- Cyber-bullying and peer on peer abuse
- Access to unsuitable video or internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading and distribution of copyright material
- The potential for excessive use that may impact on children's social and emotional development and learning.
- Risk of radicalisation

4. Many of these dangers 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-bullying and child protection policies.

Scope of the policy

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

6. 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, but is linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents or carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and responsibilities

7. The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school.

Governors

8. Governors are responsible for approving the E-Safety Policy and reviewing its effectiveness.

9. The governor with special responsibility for IT will also be responsible for e-safety. The role of the e-safety governor will include:

- regular meetings with the IT co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering and change control logs
- reporting to the relevant governors meetings.

10. Governors should take part in e-safety training and awareness sessions. This may be offered in several ways, such as attendance at training provided by the local authority, National Governors' Association, NCI or other relevant organisation and participation in school training and information sessions for staff or parents.

Headteacher

11. The headteacher is responsible for ensuring the safety, including e-safety, of members of the school community, although the day-to-day responsibility for e-safety will be delegated to the IT co-ordinator.

12. The headteacher is responsible for ensuring that the IT co-ordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

13. The headteacher will ensure that there is a system in place to monitor and support those in school who carry out the internal e-safety monitoring role.

14. The headteacher will receive regular monitoring reports from the IT co-ordinator.

15. The headteacher 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.

16. The headteacher, having overall responsibility for external relations, must ensure that parents and carers are informed of the school's e-safety policy, including the rules in relation to acceptable use.

IT co-ordinator

17. The IT co-ordinator will:

- take day-to-day responsibility for e-safety issues and have a leading role in establishing and reviewing the school's e-safety policy and related documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- provide training and advice for staff
- liaise with the local authority
- liaise with school's IT technical staff
- receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments
- meet regularly with the IT governor to discuss current issues, review incident logs and filtering and change control logs
- attend relevant meetings of governors
- report regularly to the headteacher.

18. The IT co-ordinator will receive regular updates through attendance at training sessions and by reviewing guidance documents released by BECTA, NCI, the local authority and others.

19. The IT co-ordinator will provide advice, guidance and training for staff as required. It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy.

20. The IT co-ordinator must be satisfied that:

- the school's IT infrastructure is secure and is not open to misuse or malicious attack
- the school meets the e-safety technical requirements outlined in the relevant local authority's e-safety policy and guidance
- users may only access the school's networks through a properly enforced password protection policy
- the use of the network is regularly monitored in order that any misuse or attempted misuse can be reported to the IT co-ordinator for investigation.
- monitoring software and systems are implemented and updated as agreed in school policies.

Teaching and support staff

21. Teaching and support staff are responsible for ensuring that they have an up-to-date awareness of e-safety matters and the current e-safety policy and practices.

22. E-safety should be a focus in all areas of the curriculum and other school activities and staff should reinforce e-safety messages in the use of IT across the curriculum.

23. Teaching and support staff must ensure that pupils understand and follow the e-safety policy and have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. In lessons where internet use is pre-planned, 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. Staff should monitor IT activity in lessons and extra-curricular and extended school activities.

24. Staff must be aware of e-safety issues related to the use of mobile phones, cameras and hand-held devices, monitor their use and implement current school policies with regard to these devices.

25. Staff must report suspected misuse to the IT co-ordinator for investigation.

Pupils

26. Pupils must use the school's IT systems in accordance with this policy. Pupils should:

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices, and know and understand school policies on the use of images and cyber-bullying
- 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
- not attempt to bypass the school's security systems.

27. While regulation and technical solutions are important, their use must be balanced by educating pupils to take a responsible approach. The education of 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 should be provided as part of IT, PHSE and other lessons and should be regularly revisited. This will cover the use of IT both in school and outside school.
- Pupils should be taught in all lessons to be critically aware of the materials and content accessed on-line and be guided to validate the accuracy of information.

Parents and carers

28. Many parents and carers 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 and regulation of their 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 and carers through letters, newsletters, the school's web site and parents evenings

29. Parents and carers must be informed of the school's e-safety policy, including the rules in relation to acceptable use.

Infrastructure, equipment, filtering and monitoring

30. The school will be responsible for ensuring that the school's infrastructure and 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.

31. School IT systems will be managed in ways that ensure that the school meets the e-safety technical requirements and any relevant local authority e-safety policy and guidance.

32. Servers, wireless systems and cabling must be securely located and physical access restricted. Appropriate security measures must be in place to protect the servers, firewalls, routers, wireless systems, workstations, hand-held devices, etc. from accidental or malicious attempts that might threaten the security of the school systems and data. The school infrastructure and individual workstations must be protected by up-to-date virus software.

33. All users will have clearly defined access rights to school IT systems and be provided with a username and password.

34. The master/administrator passwords for the school IT system, used by the network manager or other person, must also be available to the headteacher and kept in a secure place, e.g. the school safe.

35. The school will maintain and support the managed filtering service provided by its IT contractor, to whom any filtering issues should be reported immediately. Requests from staff for sites to be removed from the filtered list will be considered by the IT co-ordinator.

36. The IT contactor will monitor and record the activity of users and users must be made aware of this. Remote management tools will be used to control workstations and view users' activity.

37. An appropriate system should be in place for users to report any actual or potential e-safety incident to the IT co-ordinator or other relevant person.

38. There will be regular reviews and audits of the safety and security of school IT systems.

Use of digital and video images

39. The development of digital imaging technologies has created significant benefits for learning, allowing staff and pupils the instant use of images either recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available indefinitely and cause harm or embarrassment in the short or longer term. For example, many employers carry out internet searches for information about potential and existing employees.

40. When using digital images, staff should educate pupils about the risks associated with taking, using, sharing, publishing and distributing images. In particular, they should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites.

41. Staff are allowed to take images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images, which should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.

Data protection

42. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Staff must ensure that they take care at all times to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.

Communications

43. A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefits of using these technologies for education outweighs their risks or disadvantages.

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	/						/	
Use of mobile phones in lessons				/				/
Use of mobile phones in social time	/							/
Taking photos on mobile phones or other camera devices	/						/	

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Use of hand held devices e.g. PDAs, PSPs	/						/	
Use of personal email addresses in school, or on school network	/							/
Use of school email for personal emails		/						/
Use of chat rooms / facilities				/				/
Use of instant messaging				/				/
Use of social networking sites				/				/
Use of blogs		/					/	

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

45. 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. Any digital communication between staff and pupils or parents and carers (email, chat, VLE, etc.) must be professional in tone and content.

46. Users must immediately report to the nominated person the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

Acceptable use

47. The school believes that the activities referred to below would be unsuitable or inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems.

48. It is illegal and unacceptable for users to 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

- the promotion or conduct of illegal acts, e.g. 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
- the promotion of any kind of discrimination or the 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.

49. The following activities are also unacceptable and prohibited:

- using school systems to run a private business
- using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by NCI or 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 (e.g. financial or personal information, databases, computer or network access codes and passwords)
- creating or propagating computer viruses or other harmful files
- carrying out sustained or instantaneous high-volume network traffic (downloading or uploading files) that causes network congestion and hinders others in their use of the internet.

50. The following table shows other uses that may or may not be prohibited:

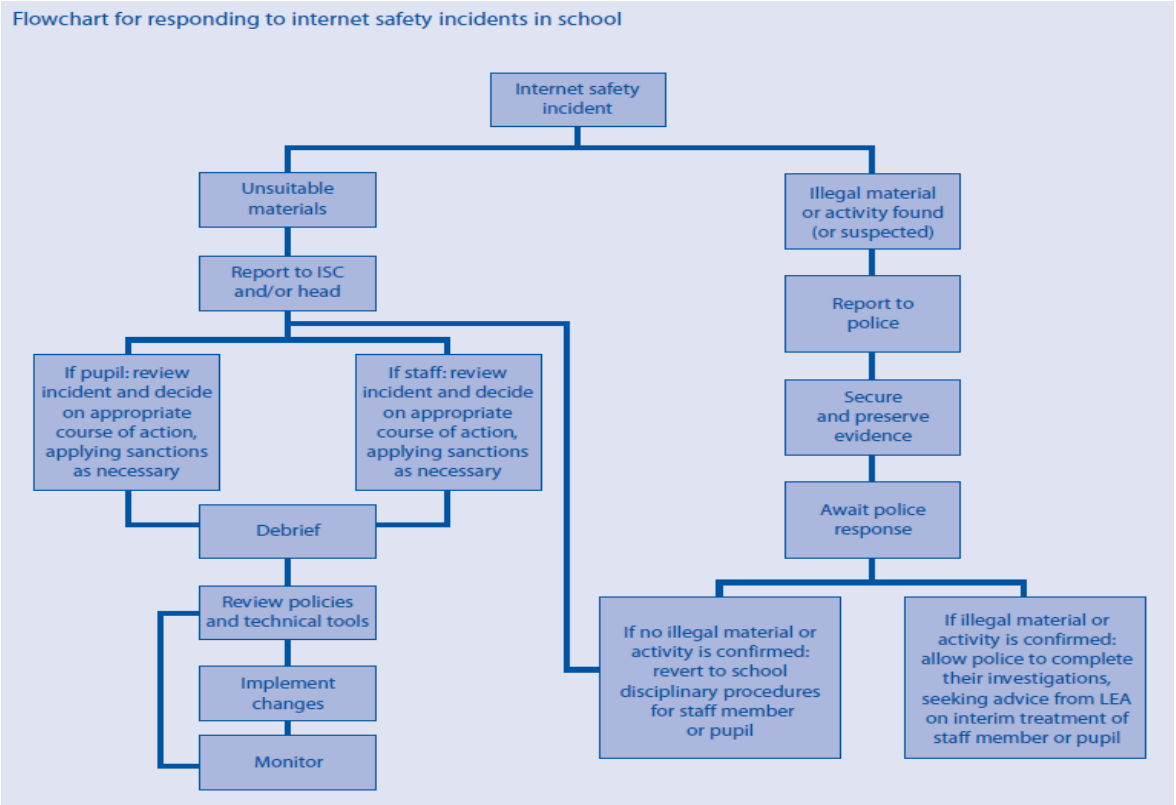
	Acceptable	Acceptable at certain times	Acceptable for nominated users	Not acceptable
On-line gaming (educational)	/			
On-line gaming (non educational)				/
On-line gambling				/
On-line shopping / commerce		/		
File sharing		/		
Use of social networking sites				/
Use of video broadcasting e.g. Youtube		/		

Responding to incidents of misuse

51. It is hoped that all members of the school community will be responsible users of IT who understand and follow this policy. However, there may be times when infringements of the policy could take place, through accidental, careless or irresponsible use or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse.

52. The flow chart below should be consulted and actions followed, in particular the sections on reporting the incident to the police and the preservation of evidence, if any apparent or actual misuse appears to involve illegal activity, e.g.

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



53. If members of staff suspect that misuse might have taken place, but the misuse is not illegal, as defined above, it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. More than one member of staff must be involved in the investigation, which should be carried out on a "clean" designated computer. The affected device should, if possible, be switched off and technical support be sought, if necessary.

54. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. 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 normal behaviour and disciplinary procedures.

Appendix 1: Staff and Volunteer Acceptable Use Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside.[1] The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure that:

- staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- the school's ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- staff are protected from potential risk in their use of ICT in their everyday work and when using social networking sites both at work and at home.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use the school's ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e–safety in my work with young people.

For my professional and personal safety, I understand that:

- the school will monitor my use of the ICT systems, email and other digital communications
- the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE, etc.) outside the school
- the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.

I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.

I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

[1] All references to academies and colleges in the template on which this agreement is based have been removed and the term 'school' is used throughout.

I will be professional in my communications and actions when using school ICT systems.

I will not access, copy, remove or otherwise alter any other user's files without their express permission.

I will ensure that when I take or publish images of others, I will do so with their permission and in accordance with the school's policy on the use of images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website), it will not be possible to identify by name or other personal information those who are featured. The school and, where necessary, the local authority have the responsibility to provide safe and secure access to technologies.

When I use any personal device in school, I will follow the rules set out in this agreement, in the same way as if I were using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.

I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.

I will ensure that my data is regularly backed up, in accordance with relevant school policies.

I will not try to upload, download or access any materials that are illegal (e.g. child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering or security systems in place to prevent access to such materials.

I will not disable or cause any damage to school equipment or the equipment belonging to others. I will immediately report any damage or faults involving equipment or software, however this may have happened.

I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school or local authority's Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.

I understand that data protection policy requires that any staff or pupil data to which I have access will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

When using the internet in my professional capacity or for personal use sanctioned by the school, I will ensure that I have permission to use the original work of others in my own work. Where work is protected by copyright, I will not download or distribute copies, including music and videos.

I understand that:

- I am responsible for my actions in and out of school
- this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in the school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in the school or in situations related to my employment by the school

- if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could be a warning, suspension, referral to governors or the local authority and, in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use the school ICT systems, both in and out of the school, and my own devices in the school and when carrying out communications related to the school within these guidelines.

Staff or volunteer name:

Signed:

Date: