An Daras
Multi Academy Trust

The Federation of North Petherwin and Werrington Schools
Member of An Daras Multi-Academy Trust

E-Safety Policy

1. Aims and objectives

Within our federation, the requirement to ensure children and young people are able to use the Internet safely is addressed as part of our wider safeguarding duty of care to which all who work is schools are bound. This policy aims to help to ensure the safe and appropriate use of all e-technologies. E-safety is not about the technologies but about people and their actions.

The development and implementation of this policy involves all stakeholders including headteacher, governors, senior leaders, classroom teachers, support staff, parents, members of the community and pupil themselves.

The risks currently identified include:

- Access through the Internet to harmful, illegal or other inappropriate materials;
- Unauthorised access to/loss of/sharing of personal and confidential information;
- Pupils being contacted through the Internet and groomed;
- Pupils sharing personal information about themselves over the Internet;
- The sharing or distribution of personal images without a person's knowledge or permission;
- Inappropriate contact with others including strangers;
- Cyber-bullying;
- Access to unsuitable or age inappropriate videos or online games;
- An inability to evaluate the quality, accuracy and relevance of information on the Internet;
- Plagiarism and copyright infringement;
- Illegal downloading of music or video files;
- The potential for excessive use which may impact on the social and emotional development and learning of the pupil.
-
- This policy outlines the procedures we have put in place and the responsibilities of stakeholders to address these areas of risk. It has been developed by a working group made up of:

- Headteacher;
- E-Safety Coordinator;
- Staff – including Teachers, Support Staff;
- Governors;
- Parents and Carers;
- Community users;

2. Scope of the policy

This policy applies to all members of the school community: staff, pupils, volunteers, parents, visitors, community users and governors who have access to school IT 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 outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

RRSA

Through this policy we, as the Federation of North Petherwin and Werrington Schools, aim to promote the UNCRC in all aspects of our work, this reflects our position as a Rights Respecting School.

E-safety relates to the UNCRC articles:

Article 13 (freedom of expression) Every child must be free to express their thoughts and opinions and to access all kinds of information, as long as it is within the law.

Article 17 (access to information from the media) Every child has the right to reliable information from a variety of sources, and governments should encourage the media to provide information that children can understand. Governments must help protect children from materials that could harm them.

Article 28 (right to education) Every child has the right to an education.

Article 29 (goals of education) Education must develop every child's personality, talents and abilities to the full. It must encourage the child's respect for human rights, as well as respect for their parents, their own and other cultures, and the environment

Article 31 (leisure, play and culture) Every child has the right to relax, play and take part in a wide range of cultural and artistic activities.'

Article 36 Governments must protect children from all other forms of bad treatment.

British Values

This policy supports the Federation's aims to embed British values at this school in the following ways:

- E-safety guidance and rules within the school ensure pupils are not exposed to radical views or discriminatory views. This ensures that the school complies with 'THE PREVENT DUTY UNDER THE COUNTER TERRORISM AND SECURITY ACT 2015'.
- Pupils are encouraged to know, understand and exercise their rights and personal freedoms and receive advice about how to exercise these safely, for example through our exploration of E-Safety in Computing and Citizenship.

Responsibilities

Headteacher and Assistant head:

- have a duty of care 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;
- 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;
- are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant;
- will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles;
- ensure the governors receive regular monitoring reports from the E-Safety Co-ordinator;

E-Safety Coordinator:

- leads the e-safety committee;
- 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 the Local Authority as necessary;
- liaises with school technical staff;
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments;
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs;
- attends relevant committee of Governors;
- reports regularly to the Headteacher;

E-safety link Governor:

- maintains an up-to-date awareness of e-safety;
- meets regularly with e-safety coordinator to oversee this policy;
- reports regularly to governors on e-safety matters;
- makes recommendations to the head/e-safety coordinator/governing body as necessary.

Technical staff:

- ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack;
- ensure that the school meets required e-safety technical requirements and any Local Authority E-Safety Guidance that may apply;
- ensure that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed;
- ensure the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- ensure that they keep 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;
- ensure that the use of the network / internet / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation;
- ensure that monitoring software / systems are implemented and updated as agreed in school policies.

Teaching and Support Staff:

- ensure that they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;
- read and have understood and signed the Staff Acceptable Use Policy;
- report any suspected misuse or problem to the Headteacher for investigation
- ensure that all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems;
- plan so that e-safety issues are embedded in all aspects of the curriculum and other activities;
- ensure pupils understand and follow the e-safety and acceptable use policies;
- ensure that pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices;
- in lessons where internet use is pre-planned ,make sure 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.

Child Protection / Safeguarding Designated Officer:

should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data;
- access to illegal / inappropriate materials;
- inappropriate on-line contact with adults / strangers;
- potential or actual incidents of grooming;
- cyber-bullying.

E-Safety Committee:

The E-Safety Committee provides a consultative group that has wide representation from the school community, with responsibility for issues regarding e-safety and the monitoring of the e-safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the E-safety Group will assist the E-Safety Coordinator with:

- the production / review / monitoring of the school e-safety policy / documents;
- the production / review / monitoring of the school filtering policy and requests for filtering changes*;*
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression;
- monitoring network / internet / incident logs;
- consulting stakeholders – including parents / carers and the pupils about the e-safety provision;
- monitoring improvement actions identified through use of the 360 degree safe self- review tool.

Students / pupils:

- are responsible for using the *school* digital technology systems in accordance with the Pupil Acceptable Use Policy;
- 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 policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / 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 / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the *school* in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events;
- access to parents' sections of the website and on-line pupil records;
- their children's personal devices in the school.

Community Users:
Community Users who access school systems / website as part of the wider *school* provision will be expected to sign a Community User AUA before being provided with access to school systems.

4. Curriculum

Within our federation, the e-safety knowledge and understanding that pupils need is planned for carefully so that it forms part of all teaching in computing and across the curriculum. Staff will reinforce e-safety messages whenever computing or the Internet is being used. Staff will need to:

- ensure that pupils know the procedure for dealing with unsuitable material that is found during an Internet search;
- ensure that whenever Internet use is planned for, best practice is followed at all times;
- supervise all pupils at all times when accessing the Internet;
- be vigilant in monitoring the content of websites that pupils are visiting;
- teach pupils how to be critically aware of the material they access via the Internet and guide them to validate its accuracy;
- teach pupils to acknowledge the source of the information used and to respect copyright when using material accessed on the Internet;
- teach at least one specific age-appropriate lesson a ½ term which focuses on e-safety including being safe online and cyber-bullying;
- ensure pupils follow the home-school acceptable use agreement.

As a federation we will carry out ½-termly e-safety assemblies and take part in Safer Internet day annually.

5. Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Kept no longer than is necessary;
- Processed in accordance with the data subject's rights;
- Secure;
- Only transferred to others with adequate protection.

Staff must 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 – passwords should not be saved to ensure accidental access cannot happen;
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media or on the school's online system or network:

- the device must be password protected;
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete;
- the names of pupils will be anonymous or only first names used.

6. Use of digital images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students / 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 eg on social networking sites;
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images must not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images;
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes;

- Care should be taken when taking digital / 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 blog that include pupils will be selected carefully and will comply with good practice guidance on the use of such images;
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs;
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or blogs;
- Pupil's work can only be published with the permission of the pupil and parents or carers.

7 Schedule for Development / Monitoring / Review

This e-safety policy was approved by the Governing Body on:	*****2015
The implementation of this e-safety policy will be monitored by the:	E-Safety Coordinator
Monitoring will take place at regular intervals:	Termly
The Governing Body will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	Annually
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:	June 2016
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	LADO, Police

The school will monitor the impact of the policy using:

- Logs of reported incidents;
- Monitoring logs of internet activity (including sites visited);
- Surveys / questionnaires of
  - students / pupils;
  - parents / carers;
  - staff;

8. Agreed use of Communication Technologies

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

	Staff & other adults				Students / Pupils			
Communication Technologies		n times	ted staff				n times	f permission
Mobile phones may be brought to school	Turned off In class				X			
Use of mobile phones in lessons					X			
Use of mobile phones in social time								
Taking photos on mobile phones / cameras				X				
Use of other mobile devices eg tablets, gaming devices					X			
Use of personal email addresses in school, or on school network								

Use of school email for personal emails								
Use of messaging apps	urposes							X
Use of social media								
Use of blogs	For educational purpose	s and under supervision						

All use of the above communications technologies must be in accordance with the school's acceptable use agreements.

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored;
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.;
- Any digital communication between staff and students / pupils or parents / carers (email, chat,) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications;
- Whole class / group email addresses may be used for pupils;
- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies;
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

9. Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes this policy and our acceptable use agreements give clear guidance for staff to manage risk and behaviour online. The core message is that all behaviour should when publishing online be conducive to the protection of pupils, the school and the individual. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. While, Ofsted's e-safety framework 2012, reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise.

Our schools have a duty of care to provide a safe learning environment for pupils and staff. The schools and local authority could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the schools or local authority liable to the injured party. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers school staff or school incidents;
- They do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the school or local authority;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

10. Guidance on what constitutes inappropriate activities

The school believes that the activities referred to in the following section would be 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. The school policy restricts usage as follows:

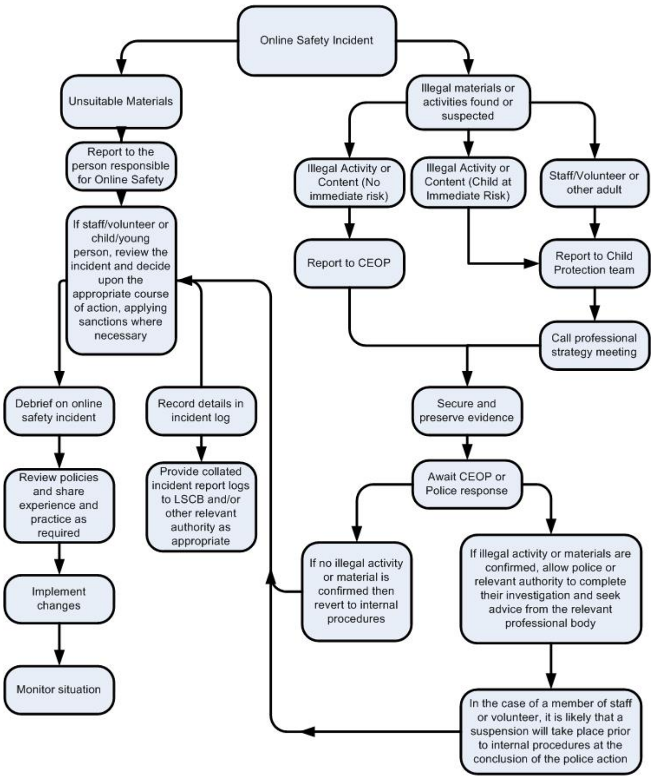
User Actions		Acceptable	Acceptable at certain	Acceptable for nominated	Unacceptable	Unacceptable and
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks,	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X

proposals or comments that contain or relate to:	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	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				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)					X	
On-line gaming (non educational)					X	
On-line gambling					X	
On-line shopping / commerce					X	
File sharing					X	
Use of social media					X	
Use of messaging apps						
Use of video broadcasting eg Youtube						

11. Procedures to follow when responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents:
If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Other Incidents:
It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority
  - Police involvement and/or action

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour;
- the sending of obscene materials to a child;
- adult material which potentially breaches the Obscene Publications Act;
- criminally racist material;
- other criminal conduct, activity or materials;

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the *school* and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

11. School Sanctions

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 / disciplinary procedures as follows or in the case of staff as directed by the headteacher.

Pupils

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

12. Appendices

In the appendices are documents use in conjunction with and to support this e-safety policy.

- Pupil Acceptable Use Agreement (KS1);
- Pupil Acceptable Use Agreement (KS2);
- Parents/Carers Home - School Acceptable Use Agreement;
- Use of digital images and videos permission;
- Staff and Volunteers Acceptable Use Agreement;
- Community users Acceptable Use Agreement;
- Record of reviewing sites (for internet misuse);
- School Reporting Log;