File: **Governors**	
Initials: **HKE**	Date: **09/2015**
Pages: **12**	
Review: **HKE**	Date: **09/2018**

e-SAFETY POLICY
September 2015

This policy links directly with Safeguarding and ICT security policies. e-Safety is the safeguarding of children in the use of electronic media in everyday life including PC's, laptops, tablets, mobile phones, webcams etc place an additional risk on our children. Internet chat rooms, discussion forums or social networks can all be used as a means of contacting children and young people with a view to grooming them for inappropriate or abusive relationships. The anonymity of the internet allows adults, often pretending to be children, to have conversations with children and in some cases arrange to meet them.

Responsibilities
Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-Safety incidents and monitoring reports. A member of the Governing Body will take the role of e-Safety Governor.

e-Safety Governor (Helen Keyworth-Edwards)
The role will include:

- regular meetings with the e-Safety Co-ordinator
- monitoring of e-safety incidents logs
- reporting back to Governors meetings

The Headteacher
The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community.

- The Headteacher 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 Headteacher will ensure that there is a system in place to allow for monitoring and support of the ICT Co-ordinator. The Headteacher will regularly check monitoring logs and systems to provide a safety net and support for those colleagues who carry out monitoring roles to ensure integrity.
- The Senior Management Team will receive regular monitoring reports from the e-Safety and ICT Co-ordinators.
- The Headteacher and the Deputy 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 (see SSCB flow chart on dealing with e-safety incidents).

e-Safety Co-ordinator (Mrs Y Fearn)
The e-Safety Co-ordinator has the responsibility for day to day e-safety and should have a good knowledge and understanding of the new technologies, together with an up to date awareness of child protection issues. The e-Safety Co-ordinator:

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents. See **Appendix 1** for e-Safety curriculum out.
- 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.
- 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.
- Reports regularly to Senior Leadership Team.

The ICT Co-ordinator/Systems Manager (Helen Keyworth-Edwards) is responsible for:
- Ensuring that the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- Monitoring of the Policy Central Enterprise (PCE) system for all hardware owned by the school.
- Ensuring that the school meets the e-Safety technical requirements outlined in the School's Security Policy and Acceptable Usage Policy (AUP) and any relevant Local Authority/Entrust e-Safety Policy and guidance.
- Ensuring that users may only access the school's networks through an enforced password protection.
- Ensuring Staffordshire Learning Network filtering is applied with the RM solution 'Safety Net Plus'. Suitable control of permissions is maintained.
- Ensuring awareness of up to date e-Safety technical information in order to effectively carry out the e-Safety role and to inform and update others as relevant.
- The production / review / monitoring of the school e-Safety policy / documents in consultation with the Headteacher.

Child Protection Officer (Yvonne Fearn (Helen Coulthard and Liz Laughlin – Deputies))
Should be trained in e-safety issues and be aware of the potential for serious child protection 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
- (nb these are child protection issues)

Teaching and Support Staff are responsible for ensuring that:
- They have an up to date awareness of e-Safety matters and of the current school e-Safety policy and practices.
- They have read, understood and signed the school Staff Acceptable Use Agreement (AUP).
- They report any suspected misuse or problem to the e-Safety Co-ordinator or ICT Co-ordinator for investigation, action or sanction.

- Digital communications with pupils (email) should be on a professional level and only carried out using official school systems.
- e-Safety issues are embedded in all aspects of the curriculum and other school activities
- Pupils understand and follow the school e-Safety and acceptable use policy.
- 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 hand held devices and that they monitor their use and implement current school policies with regard to these devices.
- In lessons where internet use is planned pupils should be guided to sites checked as suitable for their use.

Pupils

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. (Foundation and Key Stage 1 parents / carers will sign on behalf of the pupils).
- Have an 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 policies on the use of mobile phones, digital cameras and hand held / mobile devices. They should also know and understand school policies on the taking of 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 Carers

Parents and 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 the issues involved through parents' evenings, newsletters, letters, website and information about national / local e-Safety campaigns / literature.
Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Use Policy.
- Accessing the school website / on-line pupil records in accordance with the relevant school Acceptable Use Policy.

Community Users

Community Users who access school ICT systems / website as part of the Extended School provision will be expected to sign a Third party community User AUP, before being provided with access to school systems.

Learning e – Safety in the curriculum

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-Safety is an essential part of the school's e-Safety provision. Children and young people have 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 Computing / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key e-Safety messages should be reinforced as part of a planned programme.
- Pupils should be taught in all lessons to be critically aware of the materials / 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 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.
- Rules for use of ICT systems / internet will be posted in rooms and displayed on log-on screens.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

E-Safety for parents and carers

Many parents and carers have an essential role in the education of their children and in the monitoring of the children's on-line experiences. Parents can either underestimate or not realise how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about what they would do about it. The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters and / or web site.
- Parents evenings or workshops.

E-Safety for Extended Schools

The school will offer family learning courses in ICT, media literacy and e-Safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e-Safety may be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

E-Safety for Staff

Staff will receive e-Safety training to understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-Safety as a training need within the performance management process.
- 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 e-Safety Co-ordinator will receive regular updates through attendance at LA training sessions and by reviewing guidance documents released by BECTA / LA /CAS and others.
- This e-Safety policy and its updates will be presented to and discussed by staff in staff meetings or INSET days.

- The e-Safety Co-ordinator will provide advice, guidance or training as required to individuals.

e-Safety for Governors

Governors should take part in e-Safety awareness sessions, with particular importance for those who are involved in ICT / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association or other relevant organisation.
- Participation in school training / information sessions for staff or parents.

Use of Communication Technologies

Please tick ✓	Staff and other adults				Students / Pupils			
Communication Technologies These permissions may be altered by HT or designated person and reported to SMT	Allowed as in AUP	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times w. permission	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				✓				✓
Use of hand held devices eg PDAs, PSPs, IPads	✓							✓
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 e.g. staff/parent texting service		✓						✓
Use of social networking sites				✓				✓
Use of blogs	✓					✓	✓	

All users must be aware that:

- The use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the e-Safety Co-ordinator /Headteacher /ICT Co-ordinator for investigation / action / sanction.
- Monitoring software is implemented and updated.

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.
- Transfer data using secure password protected devices. (Memory sticks need to be encrypted)

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device once its use is complete.

Technical – infrastructure, equipment and monitoring

The school's responsibility for ensuring that the school infrastructure is safe and secure as is reasonably possible is defined in the ICT Security Policy.

Users should note that

- All users will be provided with a username and password by ICT Co-ordinator who will keep an up to date record of users and their usernames. Users will be allowed to change their password.
- The "administrator" passwords for the school ICT system, used by the System Manager must also be available to the Office Manager and kept in a secure place. (Deputies also have access - Curriculum side Lead TA for ICT and Admin side Admin officer).

- 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.
- Requests from staff for sites to be removed from the filtered list will be considered by the System Manager and logged with advice sought from HT as appropriate.
- School monitors and records the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools may be used by staff to control workstations and view users activity.

Unsuitable / inappropriate / illegal activities
School policy restricts certain internet usage as follows:

User Actions 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:	Unacceptable	Unacceptable and illegal
child sexual abuse images		✓
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	✓	
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 SWGfL and / 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 (eg financial / personal information, databases, computer / network access codes and passwords)	✓	
Creating or propagating computer viruses or other harmful files	✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet	✓	
On-line gaming (non educational)	✓	
On-line gambling	✓	

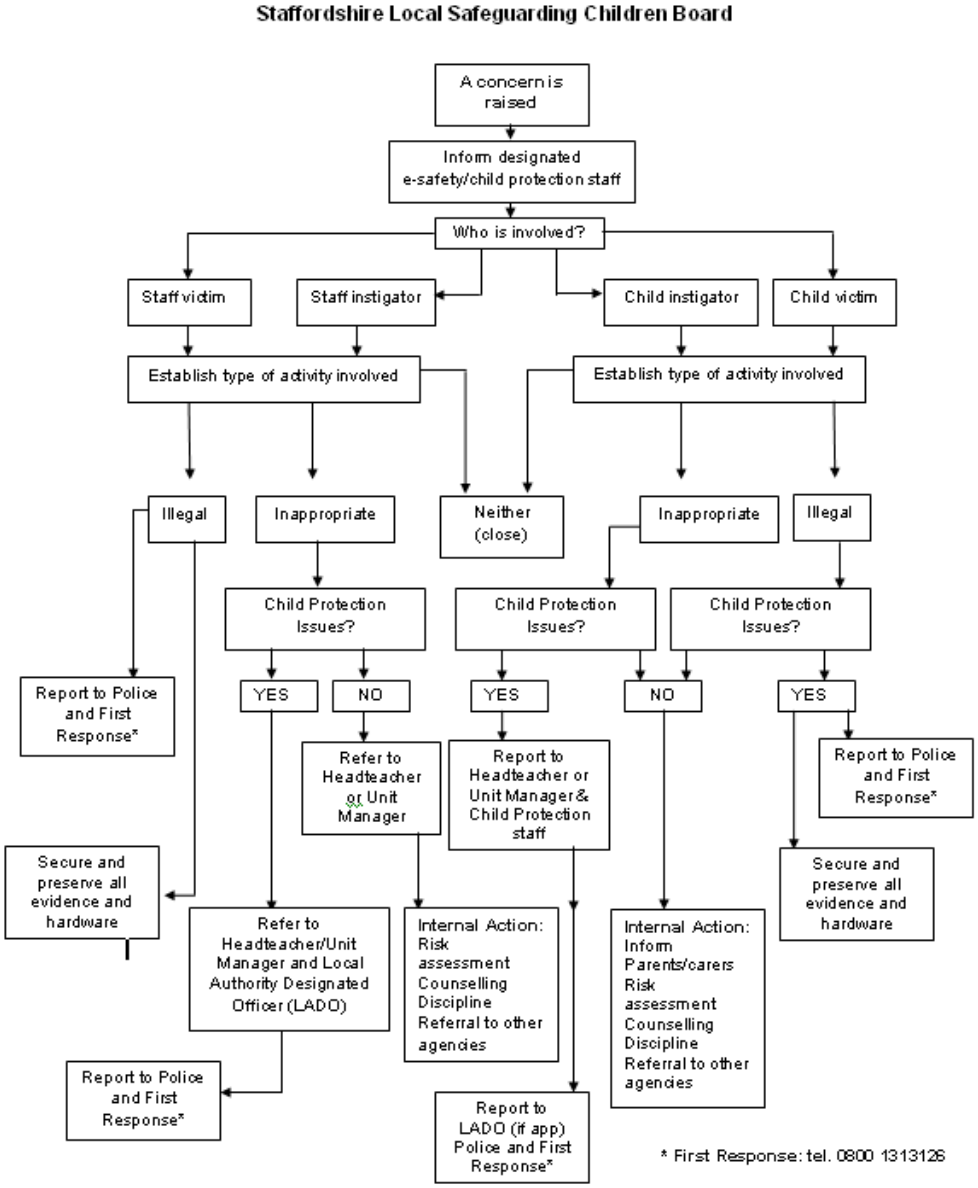
Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT. There may be times when infringements could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

Listed on the flow chart below are the responses that will be made to any apparent or actual incidents of misuse that appear 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 flow chart from the Staffordshire Safeguarding Children's board and the http://www.staffsscb.org.uk/e-SafetyToolkit/IncidentResponse/should be consulted. Actions should be in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal, it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event contact the Staffordshire Safeguarding Children's Board.

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. The Headteacher would investigate in the first instance. The Headteacher, in consultation, will decide if there is any further action required.

Sanctions
Inappropriate behaviour will be dealt with under the Disciplinary Procedures - this would apply to both staff and pupils.

Legislation (also refer to ICT Security Policy)
The school community should be aware of the legislative framework under which this e-Safety Policy has been produced. In general terms, an action that is illegal if committed offline is also illegal if committed online. Legal advice may be sought in the event of an e safety issue or situation.

Computer Misuse Act 1990
This Act makes it an offence to:
- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998
This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:
- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Not kept longer than necessary;
- Processed in accordance with the data subject's rights;
- Secure;
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988
It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system;

Monitoring but not recording is also permissible in order to:

- Ascertain whether the communication is business or personal;
- Protect or support help line staff;
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice and Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964
Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial;
- The right to respect for private and family life, home and correspondence;
- Freedom of thought, conscience and religion;
- Freedom of expression;
- Freedom of assembly;
- Prohibition of discrimination;
- The right to education.

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006
Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

See also
ICT Computer Security Policy September 2015
AUP
Computing Policy
Child Protection
Email & Internet Use Policy
Inclusion Statement
Behaviour Policy

Computing Curriculum

Aims for e-Safety

The national curriculum for computing aims to ensure that all pupils are responsible, competent, confident and creative users of information and communication technology.

Key Stage 1

- use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Key Stage 2

- use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content
- use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact

Early Years Foundation Stage - ***Laying the foundations for e-safety teaching***

Learn that staying safe online is similar to staying safe in the real world. Be introduced to the basics of online searching. Explore and comment on different types of websites with the teacher, which are pupils favourites and why? Discuss how they use the computer/tablets at home and the difference between home and school use.

Other e-safety resources to consider

Digi Duck
http://www.kidrex.org/
http://www.thinkuknow.co.uk/5_7/
The Adventures of Smartie the Penguin

Year 1

Going Places Safely - Staying safe online, ABC Searching - Simple search techniques, Keep it Private - Keep personal information private, My Creative Work - Having ownership of what is yours, Sending Email - Communication in a digital world

Other e-safety resources to consider

Think You Know resources/Hector's World
Cybersmart Resources

Year 2

Staying Safe Online - Using sites suitable for age, Follow the Digital Trail - Digital Footprints Screen out the Mean - Introduction to cyberbullying, Using Keywords - Efficient searching, Sites I like - Rating websites

Other e-safety resources to consider

Think You Know resources/Lee and Kim
Cybersmart Resources

Year 3

Powerful Passwords - The why behind passwords, My Online Community - Making connections through the internet, Things for Sale - Online advertising, Show Respect Online - Friends online and offline, Writing Good Emails - Effective communications

Other e-safety resources to consider

Captain Kara, Winston and the SMART Crew
Cybersmart Resources

Year 4

Rings of Responsibility - Showing respect online and offline, Private and Personal Information - Sharing your information with others, The Power of Words - Cyberbullying, The Key to Keywords - Accuracy in searches, Whose is it, Anyway? - Introduction to plagiarism

Other e-safety resources to consider

Think You Know Resources
Cybersmart Resources

Year 5

Strong Passwords - Creating secure passwords, Digital Citizenship Pledge - Working together, You've Won a Prize! - Introduction to Spam, How to Cite a Site - What is a citation? Picture Perfect - Digital manipulation and the implications

Other e-safety resources to consider

Think You Know Resources
Cybersmart Resources

Year 6

Talking Safely Online - Keeping personal information private, Super Digital Citizen - Working together, Privacy Rules - What are secure websites? What's Cyberbullying? - What is it and how to deal with it? Selling Stereotypes - How the media sells ideas

Other e-safety resources to consider

Think You Know Resources
CEOP Jigsaw Assembly
Cybersmart Resources