E-Safety Policy

Scope of the Policy

This policy sets outlines the role of the school in ensuring that pupils are kept safe on-line in school.
Although the school will take care to prevent pupils being exposed to risk while online and connected in school time, the school recognises that use of the Internet outside school is now widespread. Pupils therefore need educating as to the potential risk of using the Internet, and need to acquire skills and strategies to keep themselves safe.

This document:

- Identifies the key people and their roles and responsibilities.
- Outlines the strategy in which the school will endeavour to keep its pupils safe from harm, both by electronic protection, and by education of pupils and parents
- Identifies the procedures to follow in the case of an incident

Roles and Responsibilities

The Appointed E-Safety Governor is XXXXXXXXXXX
Their role includes:

- Meeting with the E-Safety Co-ordinator on a regular basis
- Regular monitoring of e-safety incident logs
- Regular monitoring of filtering/change control logs
- Reporting to relevant Governors committee meetings

The E-Safety Coordinator is XXXXXXXXXX
Their role includes the following:

- Leading the school e-safety committee
- Day to day responsibility for e-safety issues with a leading role in establishing and reviewing the school e-safety policies and documentation
- Ensuring that all staff are aware of the policy and the procedures that need to be followed in the event of an e-safety incident taking place.
- Providing training and advice for staff
- To liaise with the Local Authority and other agencies if and when required
- To work with school ICT technical staff on e-safety
- To receive reports of e-safety incidents and maintain a log of incidents to inform future e-safety policy and practice
- To meet regularly with E-Safety Governor to ensure Governing body is kept aware of current
- Attends relevant meeting (committee) of Governors to inform Governors
- Report regularly to Senior Leadership Team

Headteacher and Senior Leaders:
The Headteacher has overall responsibility for ensuring the safety of members of the school community. However, the day-to-day responsibility for e-safety will be delegated to the E-Safety Co-ordinator. The SLT will receive regular monitoring reports from the E-Safety Co-ordinator and attend the regular meeting as part of the E-Safety Meeting

The Designated person for child protection is XXXXXXXXXXXXXX
They will work with the E-Safety Co-ordinator drawing on each other's experience and expertise in order to ensure that pupils are kept safe, and should 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

E-Safety Committee
The Following people make up the e-safety committee and shall meet every half term to discuss the E-safety Co-ordinators report
Headteacher
SMT Rep
Teaching Assistant Rep
Child Protection Co-ordinator

Statement of Policy

Education for Pupils

Keeping children safe online is critically all about education. Although filters are in place to protect pupils whilst in school, this is only a small percentage of the time that a child is potentially on-line. Schools must play their part in educating pupils in how to negotiate the Internet without the safety net of filtering in place. This is the same principle as guides Stranger-Danger and Road Safety. It is about developing risk strategies and responses to threats – potential or real.

The School will provide E-Safety education in the following ways:

- A planned e-safety programme as part of ICT / PHSE / other lessons, with key themes regularly revisited covering all communication technologies where there is a safety risk
- Key e-safety messages should be reinforced as part of a planned programme of assemblies (with parents invited to share)
- Pupils should be taught in all lessons to be critically aware that not everything they access on-line is truthful or valid and be taught to check the accuracy of information
- Pupils should be included in the roll out and review process for the pupil AUP and encouraged to adopt and promote 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 and the internet will be posted in all rooms regardless of if computers are in use there, as the use of mobile devices mean that the Internet is accessible across the site
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education for Parents / Carers

Educating parents is key if children are to develop strategies to deal with the potential risks of the Internet. Parents perception of risk is often limited and badly informed. Scare stories in the media often cause parents un-necessary concerns, whilst obscuring real issues and risks. The School attempts to provide as much useful information as possible to help parents keep their children safe online outside of the school. This is open to carers and extended family such as grandparents as well.

This is done by

- Letters, newsletters, web site, VLE
- Parents evenings
- Assemblies and events

Of course all members of staff are happy to provide support to parents but they are obliged to refer any contact if they suspect that there may be e-safety concerns.

Education & Training for Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

A planned programme of formal e-safety training will be made available to staff. 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

- This E-Safety policy and its updates will be presented to and discussed by staff prior to adoption, and as part of on-going review
- The School will seek to provide the best advice on practice to support E-Safety training as required to individuals and groups

Training for Governors

- Governors should undertake e-safety training / awareness sessions both individually for nominated persons, and as a body, in order to discharge its responsibilities as in the 2012 OfSTED Handbook

*Inspectors should consider (paragraph 118); types, rates and patterns of bullying and the effectiveness of the school's actions to prevent and tackle all forms of bullying and harassment – this includes **cyberbullying** and prejudice based bullying related to special educational need, sexual orientation, sex, race, religion and belief, gender reassignment or disability.*
*The grade descriptor for outstanding includes "Pupils are fully aware of different forms of bullying, including **cyberbullying** and actively try to prevent it from occurring. They understand clearly what constitutes unsafe situations and are highly aware of how to keep themselves and others safe, including in relation to **e-safety**.*

E-Security

The School will take all reasonable steps to maintain a safe and secure environment

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the relevant Local Authority E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the E-Safety Committee (or other group).
- All users will sign an appropriate Acceptable Use Policy before using the Internet.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe)
- All users are responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by LA
- In the event of Technical Support (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).
- Any filtering issues should be reported immediately to LA

- Requests from staff for sites to be removed from the filtered list will be considered by the LA via their support mechanism for doing so
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy
- Any actual / potential e-safety incident should be reported to the relevant person/s which in most cases will include the e-safety co-ordinator unless there are concerns about their conduct in which case it should be escalated to involve SMT or the Headteacher

An agreed policy is in place "Laptop AU Policy" regarding the extent of personal use that users (staff / Pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of school.

- staff are forbidden from installing programmes on school workstations / portable devices.
- staff must only use approved, encrypted memory sticks to store/transfer information
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured, as per Data Policy

Safe Use of Digital Photographic and Video images

The use of digital imaging technologies has significant benefits to learning, allowing Staff and Pupils instant use of images that they have 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 on the internet forever as part of a digital footprint, and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. Staff should be aware of, and understand the schools policy on Staff use of Social Networks

- 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/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 taken in school, of others, without permission of the subject and the school.
- Photographs published on the website, or elsewhere that include Pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / 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
- Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers

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 take care at all times to ensure the safe keeping of any critical data, minimising the risk of its loss or mis-use. They must

- Store personal or critical 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 encryption and secure password protected devices such as USB sticks

Once data has been transferred or its use is complete the data must be *securely* deleted from the device

E-Communication

The School provides all staff with an e-mail account for use in connection with their duties. It is expected that users of the system recognise that they are representing the school in any correspondence they undertake via this system and therefore have a duty to act with due care and regard to their actions.

Users of the system should be aware of the following

- The school email system may be regarded as safe and secure. It is virus checked and monitored, and should be used in all school related communications.
- Personal e-mail accounts should be used for private communications.
- Personal e-mail accounts should not be accessed on the school systems unless permission is given to do so outside of teaching times
- E-mail and internet communications may be monitored
- All users must immediately report, to the nominated person – in accordance with the school policy, 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.
- Any digital communication between staff and Pupils or parents / carers (email, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Whole class e-mail addresses will be used at KS1, while Pupils at KS2 and above will be provided with individual school email addresses for educational use.

- Pupils will be taught about good email practices, safety issues, and how to respond to the risks attached to the use of e-mail.

Illegal and Unacceptable Internet Activity

The school believes that the activities below would be illegal, and or unacceptable in a school context and that users of the school systems should not engage in these activities. The school policies and systems restrict and forbid certain Internet usage as follows:
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 behaviours, 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 LA 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 (educational)
- On-line gaming (non educational)
- On-line gambling
- On-line shopping / commerce
- File sharing
- Use of social networking sites(see social networking policy)
- Publishing to YouTube or similar sites

Responding to incidents of misuse
It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy.

However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

All concerns regarding E-Safety either with regard to pupils safety or user misconduct should be reported to the designated person for child safety and or the Headteacher and the schedule for reporting incidents followed accordingly as for any aspect of child safety or welfare or staff misconduct.