The Grange School

E-Safety Policy

March 2018
To review March 2019

THE GRANGE SCHOOL
DAVENTRY, NORTHAMPTONSHIRE

The Grange School

E-safety Policy

The Grange School E-Safety Policy

Introduction
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 school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils to learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Radicalisation and extremism
  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 young person or the physical well-being of the child.

As with all other risks, it is impossible to eliminate those risks completely. It is

therefore essential, through good educational provision to build students' / pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / 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 / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

Governors:
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 information about e-safety incidents, as and when they arise.

Headteacher and Senior Leaders:

- The Headteacher is ultimately 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 all members of staff.
- The Senior Leadership Team is responsible for ensuring that staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Senior Leadership team 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.
- The Senior Leadership Team will be informed of any incidents relating to e-safety and will take responsibility for ensuring they are dealt with appropriately.

The ICT Subject Leader/ E-Safety Leader and ICT Technician

are responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack

- that the school meets the e-safety technical requirements
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed

  that appropriate filters and monitoring systems are in place that prevent children accessing harmful or inappropriate material.
- the school's filters are monitored routinely and updated whenever appropriate

  that restrictions are reasonable and not detrimental (over blocking) to their online learning and safeguarding
- that monitoring software / systems are implemented and updated as agreed.

  that all E-safety incidents are logged in the E-Safety folder, which is kept in the Wellbeing Room, and are reported to the Headteacher.
- that he / she keeps 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
- All users of the school network will be provided with a username and an up to date record of users and their usernames will be kept.

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 accepted the school Acceptable Use Policy
- they report any suspected misuse or problem to the E-Safety Leader and a member of the Senior Leadership Team, including any additional filters that may need to be implemented
- digital communications with pupils 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

- where students / pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

- 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 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

The school's Designated Safeguarding Leads are trained in e-safety issues and are

aware of the potential for serious child protection issues to arise from:

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

Pupils:

- are responsible for using the school ICT systems responsibly, under the guidance and supervision of school staff
- 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 school practices on the use of mobile phones, digital cameras and hand held devices and to use these devices appropriately

  will have read,understood and signed (KS2) the school Pupil Acceptable Use Agreement and parents will have read, understood and counter-signed it.

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 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:

- There is an E-safety scheme of work in place. Specific lessons on E-Safety take place termly; and always as part of the school's E-Safety Week.
- Key e-safety messages should be reinforced as part of ICT activities where appropriate throughout the rest of the year
- 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 are 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

Emails

- The official school email service may be regarded as safe and secure and is monitored. Staff and students / pupils should therefore use only the school email service to communicate with others when in school, or on school systems

- Users need to be aware that email communications may be monitored
- Users must immediately report 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 and/or parents or carers must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- 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.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Internet Filtering and Use

Our Internet provider is Schools Broadband and the filtering system used is Lightspeed Web Filter. Both organisations have met nationally defined appropriate filtering standards (See Appendices 1a and 1b). The internet filtering service will be annually reviewed.

Access to the Internet is designed to protect pupils and school personnel by blocking content that:

- promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.
- displays or promotes the illegal use of drugs or substances
- promotes terrorism and terrorist ideologies, violence or intolerance
- promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content
- displays sexual acts or explicit images
- includes illegal provision of copyrighted material
- promotes or displays deliberate self harm (including suicide and eating disorders)
- displays or promotes the use of physical force intended to hurt or kill

All users access to internet in accordance with the School's Acceptable Use Policy and Agreement and will inform the E-Safety leader if at any time they feel they have accessed inappropriate internet sites.

When inappropriate material has been accessed the Internet Service Provider will be contacted and if necessary, the Police.

Monitoring Strategies and Systems

We use a combination of physical and Internet and Web acceess monitoring.

Physical monitoring: Staff directly supervise pupils whilst using technology.

Internet and web access:Our filtering provider (Lightspeed) provides logfile information that details and attributes websites access and search term usage against individuals. School monitors this information and intervenes when necessary in the following ways:

- The ICT Technician accesses the logfile reports weekly and highlights any concerns to the E-Safety leader.
- The E-Safety leader then investigates the concern/s and contacts parents and informs the Headteacher and DSL if needed.
- The E-Safety leader plans follow up work and intervention if needed to address the concerns.
- The ICT technician will inform our filtering provider if block and monitoring lists need updating.
- The E-Safety leader will enter the concern/incident and resulting actions on the school E-Safety Log.

Date of most recent review: March 2017

Date of next review: March 2018 or sooner if required