Grateley Primary School

A School where every child becomes a lifelong learner and realises their potential.

Internet Safety Policy

Signed Chair of Governors: *Amelia Bridges*

Reviewed December 2017

Next review December 2018

Rationale

As a school we will educate and encourage pupils to keep safe through:
The content of the curriculum which:

- Will promote a school ethos which promotes mutual respect; both positive and supportive
- Will provide a secure environment and gives pupils a sense of being valued
- Will promote British Values within a strong Spiritual, Moral, Cultural and Social framework
- Will prevent radicalisation and/or or the promotion of extremist views
- Will promote the creation of a culture which helps students to feel safe and able to talk
- Will encourage pupils to talk freely about their concerns, believing that they will be listened to and valued.

New technologies have become integral to the lives of children and young people in today's society, both within school and outside of school. The internet and other forms of digital communication are powerful tools, providing children with new learning opportunities and experiences. These technologies can promote discussion, develop creativity and enable children to communicate in a range of ways, to a wide range of people.
The statutory curriculum expects pupils to learn how to create, locate, retrieve and exchange information using ICT (Information and communication technologies). In delivering the curriculum, teachers need to plan for and make use of ICT, for example, web-based resources and e-mail. Access to life-long learning and employment increasingly requires computer and communications use and pupils need to develop ICT life skills in their use.
Access to the internet and other forms of digital communication is a necessary tool for both staff and pupils within school. The purpose of internet access in school is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems.
However, these new technologies can put users, including children and young people at risk. Potential hazards they may face include:

- Cyber bullying;
- Access to harmful or inappropriate images or other content;
- Access to unsuitable videos/internet games;
- Unauthorised access to or loss of or sharing of personal information; Inappropriate communication with others, including strangers;
- The risk of radicalization or exposure to extreme ideologies;
- The risk of being subject to grooming by those with whom the make contact with online;
- The sharing/distribution of personal images without consent;
- The inability to evaluate the quality and integrity of online information;
- Plagiarism / copyright infringement;
- Data protection infringement;
- Illegal downloading of music or video files;

- Excessive, unsupervised or unsafe use of digital media may impact on the social, emotional and physical development of a young person

Many of the risks reflect the offline world and therefore this policy must be used in conjunction with all other policies, including Safeguarding, Anti-bullying, Equal Opportunities, Teaching and Learning and Health and Safety and current DfE advice including The Prevent Strategy. As with all risks, it is impossible to eliminate those risks completely. Therefore, through good education provision, pupils must learn to build resilience to risk and develop skills and confidence to face and deal with these potential pressures.

Monitoring and Review

The implementation of the E-Safety policy will be monitored by:
Amelia Allonby ***(Deputy Head Teacher and Computing and ICT leader/Anti-bullying co-ordinator)***
Rachel Dance ***(Head Teacher)***
Governing Body
Rachel Dance ***(Designated Safeguarding Lead)***
Donna Knights ***(Deputy Designated Safeguarding Lead)***

The policy will be reviewed annually, or more regularly in light of any new technological developments or incidents that may have taken place, both within the school or nationally. The school will monitor the impact of the policy by:
Reviewing the log of reported incidents Surveying pupils, parents and staff.

Scope

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who may have access to school systems, data or school equipment at any time, including hardware and software. This policy also applies all other ICT equipment brought onto the school premises by staff. On the rare occasion of any equipment being brought into school, it should be arranged with the head teacher in advance.
Any incidents arising out of the policy will be dealt with and the school will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour in school and out of school where appropriate.

Roles and Responsibilities

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

Governors

Governors are responsible for the approval of the e-safety Policy and for reviewing its effectiveness. This will be carried out by the Resources Committee.

Head Teacher and SLT

The Head teacher is responsible for the safety, including e-safety of all members of the school community, although day to day responsibility will be assigned to the ICT Co-ordinator. The SLT are responsible for ensuring the ICT Co-ordinator and other relevant staff receive suitable training or CPD in order that they can carry out their roles and train other colleagues as relevant.

ICT Co-ordinator/Deputy Head Teacher leads E-Safety within the school.

- Take day to day responsibility for e-safety issues, including providing training and advice to staff.
- Monitor e-safety incident and report regularly to the SLT.
- To liaise with the LA (Local Authority) when necessary.

All Teaching and Support Staff

- Have an up to date awareness of e-safety matters, including current policy and practices - including The Prevent Strategy;
- Report in writing any concerns over cyber/online issues to the HT/DHT.
- They have read, understood and signed the Internet Safety Policy, Safeguarding/Child Protection and associated policies.
- Understand that under no circumstances are they to provide pupils with their email/social media/mobile phone devices etc;
- Under no circumstances are they to use any social media platforms within school, apart from school based systems such as micro-librarian (monitored by teachers) and purple mash (monitoring of children emailing each other within the software platform).
- Ensure that all children in their care understand how to keep themselves safe online through ongoing class discussions, assemblies and PSHE/PDL (Personal, Social, Health and Economic Education / Personal Development Learning) lessons and internet/cyber safety lessons;
- Report in writing any suspected misuse or problems to the ICT Coordinator for investigation/action/sanction as soon as is possible and usually on the day of the concern being raised;
- Ensure pupils understand and follow the school e-safety Pupils Rules for Responsible Internet/Digital Technology Use.
- Ensure pupils have a good understanding of research skills
- Monitor ICT activity closely during lessons.
- Pre-plan internet based lessons to check sites are suitable for pupils' use - reporting and/or blocking any sites/pop-up etc that may be unsuitable (local blocking can be completed urgently through contacting the IT helpdesk).

Pupils

- Responsible for using the school's ICT system in accordance with the Internet Safety Policy.

- They need to understand and uphold copyright regulations (included in teacher planning of Computing curriculum).
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Respond appropriately to issues relating to e-safety and cyber bullying and report any concerns to an appropriate member of staff.
- Understand the importance of adopting good e-safety practice, when using digital technology in and out of school.

Parents

- Ensure that their children use internet and mobile devices in an appropriate way.
- Inform the school of any e-safety issues relevant to their child e.g. cyber bullying incidents.
- Ensure that they follow the legal guidelines for use of on-line sites, social media etc e.g. legal ages/levels of supervision.

School Wide Digital Technology Management

- The Head Teacher will delegate editorial responsibility of our school website to the Admin Officer, in liaison with the Deputy Headteacher, to ensure that content is accurate and quality of presentation is maintained.
- The website will comply with the school's guidelines. Photographs must not identify individual pupils, other than by first name and where permission has been granted beforehand. Written permission from parents will be sought before photographs of pupils are published on the school website, media or in school publications.
- Parents will be informed that pupils will be provided with supervised internet access and will sign the appropriate agreements before their child can use the internet or school technologies.
- Personal memory sticks may not be brought into school by pupils. Staff may use memory sticks for planning/work preparation, however these must be stored in lockable storage and must not under any circumstances be left out/in computers during the school day. No pupil/staff/family details may be kept on memory sticks other than the school encrypted backup.
- Responsibility for handling incidents will be given to the Deputy Headteacher in liaison with the Head Teacher.
- The 'Responsible Internet Use Statement' or 'Rules for Responsible Internet Use' signed by staff and pupils (see appendix 1 and 2);
- All staff, including teachers, supply staff, teaching assistants and support staff will be provided with the E-Safety Policy, and its importance explained.
- Parents' attention will be drawn to the policy in newsletters, the school brochure and on the school website.

The Internet

Aims of use:

To give pupils and staff the opportunities to:

- access world-wide educational resources
- to become astute and critical users of information
- participate in new initiatives such as a managed learning environment
- gather information and have cultural exchanges between appropriate pupils in other schools
- participate in staff discussions with experts in many fields
- provide access to educational materials and good curriculum practice
- communicate with the advisory and support services, professional associations and colleagues
- exchange curriculum and administration data with the Local Authority (LA) and Department for Education (DfE)

Planning and use of the Internet

- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirement.
- Pupils will be given clear objectives for internet use.
- Staff will select sites which will support the learning outcomes planned for the pupils' age and maturity.
- Approved sites must be bookmarked, listed or copied to the school intranet.
- Staff and pupils will not be allowed to access/use any public chat rooms or social media platforms (apart from teachers having access to YouTube).
- Staff and pupils will not access inappropriate sites that could put others at risk, and if inappropriate sites are encountered accidentally they will be reported to the DHT/HT immediately and will then be reported to HCC IT Help Desk. Children must then be directed away from the site and prevented from accessing this again.
- New facilities will be thoroughly tested before pupils are given access.
- Internet access will be granted to a whole class as part of the scheme of work after a suitable education in responsible internet use.
- Pupils using the Internet will be supervised by an adult.

Teaching Safe Use of the Internet

Teaching children to be safe users of the internet is of prime importance. Children before every lesson will be briefed in how to access the internet in a safer way. They will be also be reminded what to do if they see material that upsets or disturbs them, or in any way makes them feel uncomfortable.
Class teachers, following advice from the ICT Co-ordinator, are responsible for ensuring that e-safety lessons are planned across the year.

Grateley Primary School

Responsible Internet /Digital Technologies Use Statement

Staff

The computer system/network is owned by the school and is made available to pupils to further their education and for staff to:

- Enhance their professional activities including teaching, research, administration and management.
- The school's Internet Access Policy has been drawn up to protect all parties - the pupils, the staff and the school. The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any internet sites visited.
- Staff and pupils requesting internet access should sign a copy of our Acceptable Internet Use statement and return it to the ICT leader for approval.
- Access should only be made via the authorised account and password, which should not be made available to any other person;
- Staff may use memory sticks/mobile storage for planning/work preparation, however these must be kept safely remembering all the time that they may hold confidential information; any loss of such storage system may result in a breach of data protection and could result in a disciplinary action. If data storage system is compromised, staff must inform the head teacher immediately in order to minimise further risks.
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden;
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received;
- Posting anonymous messages and forwarding chain letters is forbidden;
- Copyright of materials must be respected;
- All internet activity should be appropriate for staff professional activity or pupils' education.
- The same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded or may be sent inadvertently to the wrong person;
- Use for personal financial gain, gambling, political purposes or advertising is forbidden;
- Users must access only those sites and materials relevant to their work in school.
- Users will be aware when they are accessing inappropriate materials and should expect to have their permission to use the system removed;
- Staff must not use their personal mobile phone/tablets or electronic devices in the school site (with the exception of the school office or staff room, or to make an emergency call on a school trip).
- Under no circumstances are staff allowed to use their own cameras or camera phones, or take the school cameras home.
- Staff must not give their email address/telephone numbers/or social media details to pupils or parents. Any e-contact must be made through school accounts. Any material breach of this may result in disciplinary action.

Signed: _____ Date: _____

Grateley Primary School
Rules for Responsible Internet/Digital Technology Use

Pupils

The school has computers and internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- I will not open other people's files;
- I will only use the computers for school work and homework;
- I will ask permission from a member of staff before using the internet;
- The messages I send will be polite and sensible;
- I will not give my home address, telephone number, email address or personal website details, or arrange to meet someone, unless my parent, carer or teacher has given permission;
- To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like;
- I will not use a mobile phone or electronic device on the school site
- I understand that the school may check my computer files and may monitor the internet sites I visit.

Signed by or on behalf of the pupil: _____

Date: _____

Parent/Guardian Signature: _____

Permission for Internet Access Parent/carer's permission and pupil's agreement

I give permission for access to the Internet on the terms set out in the above letter. I agree to follow the rules for Responsible Internet Use.

Signed: … … … …… …… …… …

Print name: … …… …… …… … …

Date: … …… …… …… …

Pupil Signed: … …… …… …… …… …

Print name: … …… …… …… … …… ***Class: … … …… …… …… … …***