Greatworth Primary School

E-Safety Policy

Statutory Policy	Yes	
Published on Website	Yes	
Policy Ownership	Head Teacher	Yes
	Finance & Premises Committee	No
	Quality & Standards Committee	No
	Full Governing Board	Yes
Implementation Date	March 2022	
Review Period	Annually	
Planned Review Date	March 2023	
Modifications	Reference to GDPR policy and practice p.6 CAPITA to monitor online searches p1	

Person responsible: Megan Scott (e-safety and DSL)

Writing and reviewing the e-safety policy

This e-safety policy is an add-on to the and should be viewed and used in conjunction with Acceptable Use Policy and relates to other policies including those for Computing, bullying and for child protection.

All staff at school are vigilant and are pro-active in teaching about and monitoring e-safety and this is overseen by the Head Teacher and DSLs.

Our e-Safety Policy has been written by the school, building on the Northamptonshire e-Safety Policy, the UK Safer Internet Centre and government guidance. It has been agreed by governors.

Consultation with the whole school community has taken place through a range of informal and formal meetings

The e-Safety Policy and its implementation will be reviewed annually.

Monitoring

The school will monitor the impact of the policy using

- Logs of reported incidents
- Capital It Support are responsible for setting filters and monitoring, recording and reporting inappropriate content to the Headteacher
- Monitoring of internet activity
- Internal monitoring of data for network activity
- Surveys/questionnaires of pupils, parents/carers and staff

Teaching and supporting staff are responsible for ensuring

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- They have read and understand the staff acceptable use policy
- They report any suspected misuse or problem to the Designated Child Protection Lead immediately for investigation
- All digital communications with pupils and parents/carers are on a professional level
- E-safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the e-safety and acceptable use policies
- 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 use of internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- They act as good role models in their use of digital technologies
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Pupils

- Agree and adhere to the acceptable use policy
- Are responsible for using the school digital technology systems in accordance with the pupil acceptable use policy
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents/carers understand these issues through parents' consultation evenings, newsletters and information provided on the school website.

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

Visitors

Visitors who access school systems will be expected to sign a Community Users Acceptable Use Agreement in order to be provided with access to school systems.

Teaching and Learning

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Curriculum

- E-safety is a focus in all areas of the curriculum and staff reinforce e-safety messages across the curriculum
- A planned progressive e-safety curriculum is provided as part of both Computing and PHSE alongside our Cornerstones curriculum
- Key e-safety messages are reinforced as part of a planned programme of assemblies and activities
- Pupils are taught in all lessons to be critically aware of the contents they access

online and be guided to validate the accuracy of information
- E-safety will be consistently campaigned, particularly through events such as Safer Internet Day

Internet use will enhance learning

- The school internet access will be designed specifically for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Managing Internet Access

Information system security – implemented by Capita

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with County advisors where necessary.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- Cyberbullying (the use of ICT – mobile phones, email or the internet to deliberately upset someone else) will be treated in accordance with the school anti-bullying policy.

Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Head Teacher has overall editorial responsibility and will ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Images (photographs or video/sound recordings) that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the web site 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 web site if they are on the school's media list.
- Pupil's work will be published with the permission of the pupil and parents in accordance with the school's media list.

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details or digital images of any kind which may identify them or their location. They will be made aware of the risks of publishing such images.
- Pupils and parents will be advised that the use of social network spaces, i.e., Facebook where the user age 13+, outside school is inappropriate for primary aged pupils. This will be discussed during school computing lessons.

Managing filtering

- The school will work with the LA, DfES and the Internet Service Provider, CAPITA to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Designated Child Protection Lead and added to the E-safety Incident Log.
- The ICT Technician will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing video conferencing

- Videoconferencing should be used carefully and only with designated links, i.e. a linked school.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Personal tablets or mobile phones will not be used during lessons or formal school time unless it has been pre-arranged by the teacher with approval from the Head Teacher. The sending of abusive or inappropriate messages is forbidden.
- Staff will be issued with a school phone where contact with pupils is required.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the current school internet filter provider can accept liability for the material accessed, or any consequences of internet access.

The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Cyberbullying will be dealt with in accordance with the school anti-bullying policy.
- Pupils and parents will be informed of the complaints procedure and is available on the school website.

Staff Training

A planned programme of e-safety training will be delivered to staff. This will be regularly updated and reinforced.

All new staff will receive e-safety training as part of their induction programme.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

How does GDPR relate to safeguarding?

In relation to Safeguarding, GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, children's social care and other local agencies is essential for keeping children safe and ensuring they get the support they need.

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.
- See the Information Commissions Office for further guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/

All staff in school must ensure:

- They take care and keep safe all personal data, minimising the risk of its loss or misuse.
- They send personal data securely off the school site. (See School Business Manager)
- Use password protected computers and ensure equipment is logged-off at the end of thesession where personal information could be accessed or viewed.
- Transfer or store data using encrypted and secure password devices.
- Any data transferred is used on a virus protected system which is regularly updated.
- All data is deleted from the device once transfer is complete.
- Digital Cameras are cleared before allowing off site and photographs are transferred to the school protected systems.
- Equipment that is taken off site must be checked that no personal information can be accessed.
- All devices taken off site, e.g. laptops, tablets, removable media or phones, need to be secure in a locked, safe environment and, for example, not left in cars or insecure locations.

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 be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.