WINGRAVE

Church of England School

Believe • Achieve • Enjoy

E-Safety and Technology Policy

Adopted by the GB at the meeting of the Curriculum, Community & Pupil Committee

Date of meeting: 24th November 2022

Minute number: 13

Signed by: Katie Parfoot (Chair of Governors) Signature: .....

Reviewed by		**Review Cycle**	2	**Legally Required**		**Website**	

Introduction

Technology and internet use in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to provide our young people with the skills to access life-long learning and employment.

The subject of Computing covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast-paced evolution of technology within our society as a whole. Currently the internet technologies children and young people are using both inside and outside school include:

- Websites
- Apps
- Email, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games with social media functionality
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing/uploading
- Downloading media content
- On demand TV and video
- Digital Radio and SMART televisions
- Virtual Reality Headsets and software

Whilst exciting and beneficial both in and out of the context of education, much technology, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases due to international GDPR restrictions).

At Wingrave Church of England School we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and others to help them conduct their day-to-day activities in line with our GDPR procedures. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in negative media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, regular visitors [for regulated activities] and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams,

whiteboards, digital video equipment, etc.); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices.

Breaches

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school hardware, software or services from the offending individual. For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated. Policy breaches may also lead to criminal or civil proceedings.

To protect against Ransomware or cyber attacks, school data (SIMS) is backed up by the local authority and we are currently pursuing an additional local back up system and procedure. This will provide insurance against data being held ransom as we are able to restore any systems independent of any threat.

Data protection requirements, procedures and sanctions are stated in the Data Protection Act 2018.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of technology must be reported immediately to the Headteacher and GDPR Governor, including all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications and unsolicited emails. The relevant responsible individual in the school is Matt Tomson as Headteacher unless further action is required at which point a GDPR Officer will be involved via Elaine Brown as Office Manager.

Data Security

- The school gives relevant staff access to its Management Information System, with a unique username and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff have been given GDPR training and issued with the relevant guidance documents
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Following the introduction of Sharepoint (secure online cloud storage), the use of removable storage to transport school-based sensitive data is not permitted.
- Staff should not leaving any portable or mobile equipment in unattended vehicles. Where this is not possible, it must be kept locked out of sight
- Staff should always carry portable and mobile equipment as hand luggage, and keep it under your control at all times
- It is the responsibility of individual staff to ensure the security of any personal or sensitive information contained in documents faxed, copied, scanned or printed. This is particularly important when using shared copiers/printers.

Email & Messaging

The use of electronic messages within most schools is an essential means of communication for staff, pupils and parents. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in

relation to their age and how to behave responsible online.

Staff and governors should, where possible, use a school email account for all official communication to ensure that children are protected through the traceability of all emails through the school email system. Staff or Governors who choose to use a personal or work email for school communication do so at their own risk. In addition, it is important that governors are protected against possible allegations of inappropriate contact with children. This is to help mitigate the chance of issues occurring and is an essential element of the safeguarding agenda.

Staff and Governors must remember that the nature of all communications sent electronically in the name of the school should reflect their role and the school's professional expectations.

Managing Email

- The school offers all staff & governors their own email account to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed
- Staff & governors should ideally use their school email for all professional communication.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. The school email account should be the account that is used for all school business
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses
- All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Staff sending emails to external organisations, parents or pupils are advised to cc. the Headteacher
- Pupils may only use school approved accounts/platforms (e.g. Class Dojo, TT Rockstars) on the school system and only under direct teacher supervision for educational purposes
- Emails created or received, as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your email account as follows:

    - Delete all emails of short-term value
    - Organise email into folders and carry out frequent house-keeping on all folders and archives
    - Staff must inform the Headteacher if they receive an offensive email
    - However you access your school email (whether directly, through webmail when away from the office or on non-school hardware) all the school email policies apply.

Sending emails

- Use your own school email account so that you are clearly identified as the originator of a message
- Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate
- Do not send or forward attachments unnecessarily
- School email is not for personal use.

Internet Access

The Internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material, which makes it both an invaluable resource for education, business and social interaction, as well as

a potential risk to young and vulnerable people. All Internet use is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up by senior leadership.

Children are reminded to be vigilant and cautious when using the internet at all times, reporting any concerns to a trusted adult immediately. Any incidents will then be reviewed in line with our web filtering settings on which the Headteacher, Technician and Computing Lead would collaborate.

Managing the Internet

- The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity
- Staff will preview any recommended sites, online services, software and apps before use
- Searching for images through open search engines is discouraged when working with pupils
- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources
- Pupils using or reproducing copyrighted internet materials (e.g. images, text) should be educated regarding copyright and should use references.

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience
- Do not reveal names of colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application
- On-line gambling or gaming is not allowed
- It is at the Headteacher's discretion as to what Internet activities are permissible for staff and pupils and how this is disseminated.

Computer Viruses

- All school hardware is monitored and equipped with antivirus measures.
- All files downloaded from the Internet, received via email or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.
- Never interfere with any anti-virus software installed on school equipment.
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates.
- If you suspect there may be a virus on any school equipment, stop using the equipment and contact the Headteacher and/or Technician immediately; you will be advised what actions to take and be responsible for advising others that need to know.

Virtual Reality Headsets

As a relatively new technology, staff have received specific training and guidance on the use of Virtual Reality equipment. This includes both their physical use and their internet, virtual platform connectivity.

Adults should make sure children use the headset in accordance with these health and safety warnings including making sure the headset is used as described in the 'Before Using the Headset' section and the 'Safe Environment section'.

Adults should monitor children who are using or have used the headset for any of the symptoms described in these health and safety warnings (including those described under the Discomfort and Repetitive Stress Injury sections), and should limit the time children spend using the headset and ensure they take breaks during use.

Prolonged use should be avoided, as this could negatively impact hand-eye coordination, balance, and multi-tasking ability. Adults should monitor children closely during and after use of the headset for any decrease in these abilities

Monitoring of the Policy and Review

This policy will be monitored annually by the SLT and Computing Subject Lead and changes will be made to ensure that this policy is up to date as necessary.

Further sources for professional support on online safety:

https://saferinternet.org.uk/

https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff

https://www.ceop.police.uk/ceop-reporting/

https://www.nspcc.org.uk/keeping-children-safe/online-safety/#pros

Links live as of 8.11.22