ST PETER'S CE PRIMARY & NURSERY SCHOOL WEM

'Underpinned by our Christian values, we create a happy, caring environment. This empowers each and every unique person to dream, believe, achieve and flourish.'

'In the same way, you should be a light for other people.
Live so that they will see the good things you do'

Matthew 5:16 (ICB)

ACCEPTABLE USE OF ICT POLICY SEPTEMBER 2021

Reviewed by: S Price, September 2021

Date of next review: September 2024

ICT 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, at St Peter's we need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.
At St Peter's we have an Acceptable Use Policy which purpose is to safeguard and promote the welfare of staff and pupils.

Internet

Whilst ICT is exciting and beneficial in and out of education, not all web based resources are well policed. All users need to be aware of the range of risks associated with the use of these online resources and their individual responsibilities relating to the safeguarding of children and themselves, in school and at home.

Educating pupils on the dangers of technologies that maybe encountered outside school is done as part of the e-safety curriculum. Pupils are aware of the impact of cyber bullying and know how to seek help if they are affected by any form of online bullying. Parents are also invited to attend e-safety awareness sessions.

Managing the Internet

- The school maintains that pupils will have supervised access to internet resources through the school's fixed and mobile internet technology. All staff will preview any recommended sites before use.
- Raw image searches are 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.

Internet Use

- Staff must not post personal, sensitive, confidential or classified information online.
- Staff must not reveal names of colleagues or pupils or any other confidential information acquired through your job on any social networking site or blog. This includes photographs.
- When using a social networking site, such as Facebook, staff need to remember that they have a confidentiality clause in their working contract. If they wish to communicate with another member of the school community they need to use the more private email facility. (See Social Networking Policy)
- It would be an extremely serious disciplinary issue if staff were to post photographs of children without their parents' permission due to data protection regulations.
- On-line gambling, viewing of inappropriate material or gaming is not allowed on any school owned equipment at any time.
- Pupils at St Peters' are too young to use social networking sites, such as Facebook (the legal age limit is 13 year old). However, we recognise children could be accessing the sites at home, and so provide e-safety information as necessary to ensure privacy levels are high and children are aware of the risks.

Personal Data

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person to cause harm or distress to an individual. Consequently, this could potentially damage the reputation of St Peter's Primary School.

- Everybody in school has a shared responsibility to secure any sensitive information and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.
- Staff must keep all school related data secure, including all personal, sensitive, confidential or classified data. It is the responsibility of individual staff to ensure the security of this information contained in documents faxed, copied or printed too.
- Sensitive electronic data must be stored on encrypted equipment (this includes flash drives).
- Staff received GDPR training following its introduction in May 2018.

Security

A breach or suspected breach of policy by a School employee, contractor or pupil may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

Staff should be aware that any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure.

Software security

- Any security breaches or attempts, loss of equipment and any unauthorised misuse or suspected misuse of ICT must be immediately reported to senior management (Business Manager or Headteacher).
- To minimise virus risk, staff and pupils should not bring work from home to school using portable memory sticks, unless specifically issued for the purpose with acceptable levels of encryption.
- Staff should ensure that any school information accessed from their own PC or removable media equipment is kept secure, making sure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage and keep it under control at all times and avoid leaving it in unattended vehicles. Where possible it should be kept out of sight.

Password security

- Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone.
- Pupils are expected to keep their passwords secret and not to share with others, particularly their friends.
- Staff and pupils are regularly reminded of the need for password security.
- User ID and passwords for staff and pupils who have left the school should be removed from the system within 3 months.

Disposal of redundant ICT Equipment

All redundant ICT equipment is disposed of via an authorised agency.

- A signed transfer document for the acceptance of responsibility for the destruction of any data is required.
- Any equipment that may have held personal data will have the storage media overwritten multiple times to ensure it is irretrievably destroyed.
- The School maintains a comprehensive inventory of all its ICT equipment including a record of its disposal.
- Any redundant equipment being considered for sale or gift will have been subjected to a recent electrical check.

E-mail

The school gives all staff (who require one) their own e-mail account to use for all school business as a work based tool in order to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.

- It is the responsibility of each account holder to keep the password secure. 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 e-mail addresses.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Pupils are introduced to e-mail as part of the Computing Curriculum.

- E-mails created or received as part of your 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 e-mail account as follows:
    - Delete all e-mails of short-term value.
    - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives.

Policy updated by Sophie Price (Computing Lead)
September 2021
Policy to be reviewed: September 2024

Appendix 1

School Policy in brief

At St Peter's we have an Acceptable Use of ICT Policy adapted from the LA model policy.

Protected and restricted material must be encrypted if the material is to be removed from the school.

- At St Peter's we use encrypted flash drives for this purpose and limit such data removal.
- At St Peter's we use S2S to securely transfer CTF pupil data files to other schools.
- At St Peter's we follow LA guidelines for the transfer of any other internal data transfer, using Shropshire Learning Gateway.

Protected and restricted material must be held in a lockable storage area or cabinet if in an un-encrypted format (such as paper)

- At St Peter's we store such material in lockable storage cabinets.
- At St Peter's all servers are managed by checked staff.
- At St Peter's we use follow ETS back-up procedures for the office server.
- At St Peter's we use ETS for disaster recovery on our admin server.

Disposal: Protected and restricted material electronic files must be securely overwritten and other media must be shredded, incinerated or otherwise disintegrated for data.

- At St Peter's we use the Authority's recommended current disposal firm for disposal of system harddrives where any protected or restricted data has been held.
- At St Peter's paper based sensitive information is locked away securely until removed from site and shredded by Data Shred.
- Work laptops used by staff at home if used for any protected data are brought in and disposed of through the same procedure.
- Super Users with access to setting-up usernames and passwords which enable users to access data systems e.g. for email, network access and SLG access are controlled by the LA processes.
- Security policies are reviewed and staff report any incidents where data protection may have been compromised.

This Policy is available to all staff in hard copy and electronically (Policy folder on Staff Shared 'k drive'). All new staff are given a copy at induction. It is made clear that any breach of this policy by a school member of staff will result in disciplinary action.