St Peter's Brafferton
C of E (VA) Primary School

Small school, big heart

As a church school, our vision is for each child to have a love of learning, hope, confidence, wisdom and respect for all.

'Life in all its fullness'

John 10:10

Acceptable Use Policy– ICT and E Technology Staff, Governors and visitors

Introduction

ICT in its many forms - email, the internet, cloud-based technologies and mobile devices- are now part of our daily lives. This policy is designed to ensure that all members of staff and visitors on school business are aware of their professional responsibilities when using any form of ICT and the related technologies.

Scope

This policy is specifically for staff, governors and visitors in school. Pupil use of ICT is detailed in the 'online safety' policy.

Aims

- To ensure all staff and governors use IT safely
- To ensure we are GDPR compliant and we adhere data protection laws

Principles

All staff, Governors and visitors on school business:

- Must only use the school's email, internet and intranet and other related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body. Individual employees' internet and other related technologies can be monitored and logged and can be made available, on request, to their line manager or Headteacher.
- Must only use approved, secure email systems for any school business.
- Must not browse, download or send material that could be considered offensive, and should report any accidental access of inappropriate materials to their line manager.
- Should not use school information systems or resources (e.g. cameras, laptops, memory devices) for personal purposes without specific permission from the Headteacher; they should only be used for professional purposes.
- Are not permitted to use personal portable media for storage of school related data/images (e.g. USB stick).
- Should ensure that personal data (such as data held on Scholarpack) is kept secure and is used appropriately, whether in school, taken off school

premises, or accessed remotely. Careful consideration must be given if personal data has to be accessed at home- this must be done confidentially and the screen never left unattended.

- School laptops should only be taken off site if they are password protected.
- Are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, including when on external trips/visits. With the written consent of parents (on behalf of parents) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment. Digital images are easy to capture, reproduce and publish and, therefore, must not be misused.
- Will make every effort to comply with copyright and intellectual property rights.
- Should ensure that their use of cloud-based technologies, including social networking sites, such as Facebook, Twitter, Instagram, Snapchat and Myspace, does not question or bring their professional role into disrepute.
- Members of staff are advised to consider, and set appropriately, their privacy settings on such sites.
- Should consider the appropriateness of images and material posted. Once posted online, a message, photo or video clip can be freely copied, manipulated and circulated and will potentially exist forever.
- Should only communicate with parents via Class Dojo (quiet hours must be put on) and pupils via Teams (if working remotely).
- See Appendix 1 for accessing personal information via the Cloud
- Are not permitted to contact or communicate with pupils, parents or conduct school business using personal email addresses or telephones, without specific permission from the Headteacher.
- Should not give out their own personal details, such as telephone/mobile number or email address, to pupils.
- Must ensure that all electronic communication with pupils and staff is compatible with their professional role.
- Will report any incidents of concern regarding staff use of technology and / or children's safety to the Headteacher or Designated Deputy Lead professional in line with our school's Safeguarding policies and procedures.

Monitored by: FGB
Date adopted: February 2023
Next review: February 2025
Date of next review: 2 yearly

Appendix One - Accessing cloud services on personal devices

Introduction

As remote working continues to develop, there has been a move by many organisations to transfer their locally held data into the cloud, enabling access by any internet connected device, anywhere in the world. This brings many benefits to the school, including being able to access data promptly, individuals can use a device of their own choice, and making financial savings as we do not have to provide our own devices to users.

However, with this enhanced access and benefits comes a high level of risk that the school needs to consider and mitigate through the use of technical controls, expected behaviours and supporting policies. This policy aims to provide the framework for adequate management of the risks posed should users access school systems through a non-school provided device.

Personal Devices

We identify a personal device as any electronic device that has not been provided by us and can be used to access and process personal data, including data accessed from the cloud through an internet connection. This includes, but it not limited to:

- Laptop or PC
- Notebook
- iPad or tablet
- Smartphone

Use of the device must be limited to the individual user, and not be shared resources (e.g. a family device).

Permitted Activity

Whilst using their own devices, users are permitted to access, review and process personal data within the school system in which it is held. Users must only access data they are entitled to in order to fulfil their duties.

It is not permitted for any school data to be downloaded and saved onto any personal device under any circumstances. All school data must remain within the defined systems to ensure it remains secure, available to all authorised personnel and held within our records management system for its full lifecycle, including secure destruction in line with our retention schedule.

By retaining data within school-controlled systems, in the event of an individual exercising their rights as detailed in the UK GDPR; particularly with the right to access (Subject Access Request), the searching criteria to meet a request will not require users to search their own devices for evidence of personal data that may have been stored.

Printing of any personal data to home printers is strictly forbidden. The storage and confidential disposal of paper documents cannot be easily managed and guaranteed when taken off the school site.

Device Security

Anti-virus and software security patching

The range of devices currently available all present different levels of ability to apply appropriate security and protection to the equipment. It is therefore the responsibility of the user to ensure that all available protection and security is applied. Specialist advice should be sought where appropriate.

We require that any device used for accessing school systems in the cloud must have adequate anti-virus software. The software should be installed, configured and maintained by a suitably qualified or experienced person. All available updates must be applied in a timely manner.

Out of date software (including operating systems) can provide vulnerabilities that can be exploited by unscrupulous hackers. All software installed on devices that is going to be used to access school data must be operating at the most up to date version with all security releases applied. All software should be configured and maintained by a suitably qualified or experienced person for the full period that they are used to access school data.

Password/PIN protection

All devices must be secured by a unique password or security pin to ensure that access to the device is limited to the named user permitted to access the school's personal data. Devices that lack the ability to enforce this level of security must not be used to access school data.

Data on personal devices is unlikely to be encrypted, and therefore particularly vulnerable if lost or stolen. Having a robust password or PIN in place provides an additional layer of protection.

Personal applications (apps)

Users are asked to be mindful of the apps installed on personal devices that are used to access school data. Some of these apps may have enhanced privileges and tracking within them that monitor use of the device and other items that are being accessed. This should be detailed in the application's terms and conditions and the user should seek assurance that this risk is being effectively managed.

Equipment disposal

When a device being used to access school information is disposed of, it is the responsibility of the user to ensure that no records or school data have found their way onto the device, either accidently or for a temporary purpose, prior to surrendering it as a part of an upgrade process, at point of resell or for permanent disposal through the WEEE (Waste Electronic and Electrical) process. Specialist advice should be sought where appropriate.

Physical security

Users should ensure any device used to access school data is kept safe and secured to prevent theft or damage. This includes actions such as not leaving devices overnight in cars, unattended in public spaces, or transported without sufficient protection to prevent accidental damage.

System and Accounts Security

When accessing data held in the cloud via an internet connection (e.g. Microsoft 365), users must ensure that their account is closed when not in use by logging out of the system. It is not permitted for accounts to be left open when not in use, if accessing school systems.

Users are responsible for ensuring any internet connection used to access school data is secured through the use of access controls, such as using a designated username and password. Unsecured network connections (Wi-Fi or hot spots) must not be used, and devices must be configured to prevent automatic connection to unknown networks (e.g. cafes, shopping centres, library etc.).

Data Breaches

In the event of a data breach users must follow the process detailed in the Information Security policy and report any suspected breach immediately.

Users are asked to be mindful of the following situations in which the risk of a data breach increases:

- Systems are not shut down appropriately when not in use, leading to unauthorised access of school data.
- Personal devices are shared with family, friends, or partners leading to unauthorised access of school data.
- Documents and files are downloaded onto shared devices, and then become accessible to other users of the device.
- Passwords or security PINs are shared with others (e.g. family and partners) leading to unauthorised access of school data.
- Inadequate management of security and software updates leaves a vulnerability to a virus or hack. Once unauthorised control of a device is established it is difficult to identify and remove.
- Disposal of devices that have not been adequately assessed and the permanent removal of any school related data prior to surrender.

Authorised Access

Access to school systems using personal devices is only permitted whilst the user has authorisation to do so. In the event that the user leaves the employment of the school; or the relationship terminates for third parties and contractors; access should not be attempted. To do so would be treated as a data breach and investigated as such.

It is a criminal offence under Section 170 of the Data Protection Act 2018 to knowingly access data that you are not entitled to or after you have left our employment.

Exemption Process

An exemption to any element of this policy can only be authorised by the school's Senior Information Risk Owner (SIRO). Authorisation will only be given where there is a clear business need and following a full risk assessment to ensure risks are mitigated.