Accessing Cloud Services on Personal Devices

Introduction

This Accessing Cloud Services on Personal Devices policy governs the use of personal devices to access the personal data held in Cloud based systems and processed by the school.

As remote working continues to develop across all organisations, software developers have taken steps to ensure access to data is readily available and without the constraints of being held within a restricted network. 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.

Being able to access data promptly; the financial savings for not having to provide devices to all relevant personnel; and individuals being able to use devices of their choice are all benefits that Cloud computing has brought to schools.

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.

This policy should be read in conjunction with the other policies in the School's Information Governance policy framework.

Scope

All policies in Waverley's Information Governance policy framework apply to all school employees, governors, any authorised agents working on behalf of the school, including temporary or agency employees, and third party contractors. Individuals who are found to knowingly or recklessly infringe these policies may face disciplinary action.

The policies apply to all personal data and any operational data that is classified as 'sensitive or confidential' that is held in in one of the schools systems and accessed through a non-school provided device.

Personal Devices

The School identifies a personal device as any electronic device that 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/PC
- Notebook
- iPad
- Smart Phone

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

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 individual to ensure that all available protection and security is applied. Specialist advice should be sought where appropriate.

The School requires that any device used for accessing school systems in the Cloud must have adequate anti-virus software where available. 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 are 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 named individual permitted to access the schools personal data. Devices that lack the ability to enforce this level of security must not be used for access school data.

Data on personal devices is unlikely to be encrypted, and therefore particularly vulnerable if lost or stolen. A robust password would provide an additional layer of protection.

Personal apps

Individuals are asked to be mindful of the apps installed on personal devices that they use to access school data. Some of these apps may have enhanced privileges and tracking within them that monitors use of the device and other items that are being accessed. This should be detailed in the apps terms and conditions and the individual should seek assurance that this risk is being managed.

Equipment disposal

When a device being used to access school information is disposed of, it is the responsibility of the individual, 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

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

Email and Internet Activity

Inappropriate use

The School does not permit individuals to use school email accounts to send, forward, or solicit emails that in any way may be interpreted as insulting, disruptive, or offensive by any other individual or entity. Access to websites that contain similar content is also not permitted when obtained via school systems. Full details of what is deemed inappropriate can be found in the Acceptable Use Policy.

Use of personal email accounts

The School does not permit any individual to use personal email accounts when processing personal data from the school, and therefore information cannot be sent to private email accounts for accessing outside of the school systems.

System and Accounts Security

When accessing data held in the Cloud via an internet connection (e.g. Microsoft 365), individuals must ensure that their account is closed when not in use but logging out of the system. It is not permitted for access to accounts on any of the schools system to be open when not in use.

Individuals are responsible for ensuring any internet connection used to access school data must be secured through the use of access controls (a specific user name 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.).

Permitted Activity

Whilst using their own devices, individuals are permitted to access, review and process personal data within the school system with which it is held (e.g. Outlook when responding to an email).

It is not permitted for the 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 the schools records management system for its full life cycle; including secure destruction in line with the schools 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 individuals 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.

Data Breaches

In the event of a data breach individuals must follow the process detailed in the Information Security Incident Management Reporting Policy. The risk of a data breach increases in the following situations:

- Access to systems is not closed appropriately when not in use
- Personal devices are shared with family/friends/partners
- Documents and files are downloaded onto share devices, and then become accessible to other users of the device.
- Passwords/security PINs are shared with others (e.g. family and partners); leading to the potential of unauthorised access to devices
- Inadequate management of security and software updates leaves a vulnerability to a virus/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.

Individuals are therefore encouraged to be mindful in all these situations.

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. For example, adequate mitigation measures to protect any personal data processed could include a strict requirement for the relevant staff member to delete the data from their device after use and confirm in writing to the SIRO once complete.

Authorised Access

Access to schools systems using personal devices is only permitted whilst an individual has authorisation to do so. In the event that the individual 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 an information security incident (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 the employment of that employer.

Dated: 1 November 2021