Cherwell College Oxford

Department for Education (DfE) registration: 931/6016; DfE Social care unique reference number: SC473682

USING YOUR OWN DEVICE POLICY – for workforce

This policy is to be read in conjunction with the school's e-Safety policy, available from the school's website.

Purpose

The College must ensure that adequate organisational and technical measures are in place to prevent a breach of data security as a statutory obligation under the Data Protection Act but also to protect its valuable intellectual property and commercially sensitive information. This policy's core purpose is to balance the data security risks with the operational benefits arising from the widespread use of Cloud-based consumer applications and staff owned devices.

Scope

The policy covers all College workforce with access to College IT networks, databases and systems. Whilst its requirements will be relevant to the use of any personally-procured app or device, it is assumed that College owned and provided equipment and services will always be configured to a standard consistent with the latest College information security requirements. College issued devices and applications must be used by staff in accordance with the Acceptable Use (see e-Safety Policy) and other relevant policies.

Devices and applications acquired by staff personally and only used for personal purposes (i.e. not used to access, store or transmit College data) fall outside the scope of this policy. Digital equipment, devices and apps come into scope when used to handle College data as a risk then arises of loss, disclosure or inappropriate use of College data. Staff using their own devices or apps for work purposes, should make themselves aware of this policy's requirements.

Definitions

- **Device** – fixed or mobile computing equipment (e.g. server, desktop PC, laptop, tablet, smartphone) or any equipment capable of digital data storage (e.g. USB key/memory stick, disk drive, media player, CD/DVD, digital tape).
- **Application (app)** – software used to perform a particular function that may be paid for, free-to-use, open-source or personally written. It may run locally and/or from a remote location and accessed as a web-service (Cloud). The app may be available on one or more personal and/or corporate owned devices.
- **Information security**: the preservation of the confidentiality, integrity and availability of information.
- **Information**: data which has meaning.
- **Information asset**: all data with meaning that can be exploited to advance the College's objectives or confer competitive advantage.
- **Sensitive data**: data which includes elements requiring some form of restriction of its availability. This normally includes personal information or data with commercial value to the College.
- **Handling data** – the accessing, storing or transmission of data. This includes accessing the web via College networks.

Legislative context

The College must meet its obligations under the Data Protection Act which governs the security, processing and retention of personal data.

Cherwell College Oxford

Department for Education (DfE) registration: 931/6016; DfE Social care unique reference number: SC473682

Principles

All staff using their own apps or devices to access, store and transmit College data are expected to be aware of basic information security good practice. It is a requirement that they have read and understood the College's e-Safety and Data Protection policies.

- **Do not use personal apps or devices for storing, accessing or transmitting personally identifiable or commercially sensitive information**
  The College has determined that the benefits of allowing staff to use their own apps and devices under appropriately controlled conditions justify the information security risks involved. However, these benefits arise from the convenience and productivity enhancements of being able to access personal calendars, emails, contacts and documents containing less sensitive data and should not extend to handling highly sensitive or commercially confidential data. Staff should therefore comply with the principle that the use of their own apps and devices is appropriate for activities that help them "keep in touch with the office" but not for the handling of sensitive information. The boundary between the two categories cannot be specified but staff must seek the advice of their line manager if they are unsure.

- **Device functionality and information security threats are constantly changing so the rules will be updated frequently**
  As technical requirements and solutions will change over time and new information security risks will emerge constantly, the requirements and criteria for the issuing and use of apps and devices will change frequently. The guidelines are therefore included in this policy and are subject to change from time to time.

Procedures

When using their own apps or devices to access, store, manipulate or transmit College data, all staff must comply with the following basic measures:

- Configure smartphone and tablet devices to highest available password setting. Four digit passwords are not considered sufficiently secure and most devices will support passwords of at least six digits.
- Staff owned devices that are also used for personal purposes should not be used to download personal or commercially sensitive College data.
- Personal or commercially sensitive College data should only be transmitted using College provided devices and in an appropriately secure fashion.
- Personally acquired applications, file stores and cloud based data repositories must not be used to manipulate, transmit or store College data.
- Any device or application procured at the College's expense must be acquired via the normal IT equipment/software purchasing processes.
- Smaller mobile devices such as mobile phones and tablets that are used to synchronise with College outlook accounts or access College data should not be shared with other non-College users (such as family members).
- Staff must report the loss of any personally owned device to IT Services if it is within the scope of this policy so the risk of a data breach can be assessed.