# BEAUCHAMPS HIGH SCHOOL

Beauchamps Drive, Wickford, SS11 8LY
Headteacher: Mathew Harper BA Hons, NPQH

# Data Handling Security Policy

**School Policy/Procedure No: 71**

*Last Reviewed: December 2020 Last Amended: December 2020 Next Review: December 2021*

Beauchamps High School is required to manage IT equipment, removable storage devices and papers, in the office, in transit and at home or other work locations in accordance with the General Data Protection Regulations (2016) and Article 8 of The Human Rights Act 1998.

**General rules in complying with Data Protection law:**

- Stakeholders must take responsibility for the security of the equipment allocated to them and that is in their custody.
- When stakeholders are physically transporting school data outside of our premises, on any medium, they must take steps to keep it secure.
- Official-Sensitive data must not be left unattended in a vehicle and it must always be kept out of sight.
- Stakeholders must take appropriate steps to secure our data at home and other organisations' premises.
- If working with school data on unapproved unmanaged equipment, the data must be removed when finished.
- If stakeholders are taking Official-Sensitive information out of the school, it must be recorded.
- Stakeholders must make sure that conversations discussing sensitive data are only audible by an appropriate audience.
- Stakeholders must not allow anyone access to their IT equipment through their IT account.
- Stakeholders must not use any equipment to store our business data that has not been approved.
- Stakeholders must not allow unauthorised people to be able to view information on their IT equipment display.
- If stakeholders use Outlook Web Access from an unmanaged device they must not save their password in the browser.
- Stakeholders must always use an approved secure method of disposing of physical documents and data storage devices.
- Stakeholders must return all equipment which has been issued to them by the school prior to leaving their employment.
- Stakeholders must report as quickly as possible if your equipment is lost or stolen and assist with any investigation.
- Stakeholders must ensure that both school and personal portable devices, such as laptops and mobile phones, are secured with a passcode and where possible a biometric device such as a fingerprint reader or Face ID.
- Stakeholders must keep your portable equipment clean and serviceable, including keeping it charged.

- Stakeholders must not take any of the school's equipment abroad unless they are travelling in a business capacity with approval.
- Stakeholders must not give their portable equipment to another person if they are not using it.
- Care should be taken when using Microsoft 365 at home on personal equipment to ensure other members of the household do not accidentally log in as a stakeholder. Setting up separate accounts for users on shared devices will keep log in details separate.
- Stakeholders should always lock their computer when away from the screen. This includes PCs in school and mobile phones and laptops inside and outside of school.
- Stakeholders should turn off preview of emails on device lock screens.
- Stakeholders should avoid the use of mobile storage devices in favour of Microsoft 365 storage services, such as OneDrive, Teams and SharePoint. However, where mobile storage devices, such as USB drives are necessary they should be encrypted before use.

**Note:** All data on Data Handling Security stored in school is only shared in accordance with the school's Privacy Notice