



# BEAUCHAMPS HIGH SCHOOL

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



## Data Handling Security Policy

School Policy/Procedure No: 71

*Adopted/Last Reviewed: July 2018*

*Last Amended:*

*Next Review: July 2019*

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 for longer than 10 minutes 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 all security functions are enabled on your portable equipment, such as pin codes and password access
- 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

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