DULWICH COLLEGE
FOUNDED 1619

DATA PROTECTON: DATA SECURITY POLICY

Introduction

1. Dulwich College is a data controller for the purposes of the European Union General Data Protection Regulation ("GDPR") and the Data Protection Act 2018. It has issued various privacy notices setting out the categories of individuals' personal data processed by the College, the purposes for which it is processed and the rights of data subjects.

2. This Policy sets out the College's data security principles for personal data and the current protocol for the storage of data electronically. It should be read in conjunction with the College's:

   - Privacy Notices for Pupils, Parents and Alumni;
   - Privacy Notices for Staff, Governors and other Non-Executive Officers, and Job Applicants;
   - Privacy Notices for the Commissariat (School shop), Sports Centre Members, Events and Foundation Schools' Coach Service;
   - Record of Data Processing Activities (Article 30 GDPR);
   - Data Protection Policy; and
   - IT Acceptable Use Policy for Staff.

Data Security Principles

3. Access to personal data about current, past or prospective College and Foundation school pupils, alumni, parents/guardians, staff, prospective staff, contractors and referees, members of the public using the College facilities, donors, volunteers, fundraisers and Commissariat customers is provided to members of staff who require access to that data to perform their duties and responsibilities.

Personal Data held in hard copy

4. Personal data held in manual files is only accessible by authorised individuals and, where it is confidential or sensitive, is kept in locked filing cabinets when not in use. The physical security of the College premises is checked regularly by authorised personnel.

5. Paper-based copies of personal data are disposed of in a secure manner (either by shredding or by placing in Lombard Recycling sacks).

Personal Data held electronically

6. All data on the College networks is protected by:

- an IT Acceptable Use Policy for Staff which sets out the basis upon which staff may access the College's IT Systems, use the email system, electronic file storage, security of devices, copyright and data protection and monitoring of IT systems (and a similar policy that applies to pupils);
- a firewall configuration;
- anti-virus software that runs on servers and workstations and is updated automatically;
- tracked access to all network resources;
- encryption of certain data across public networks (such as bank cardholder data);
- use of passwords;
- compliance with Payment Card Industry Data Security Standard ("PCI DSS") and the implementation of comprehensive requirements for enhancing security of payment card account data in accordance with industry standards from time to time (https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf) (other than when used in conjunction with the College Wi-Fi system);
- regular testing of security systems and processes; and
- the daily back up of data.

Password Protection

7. Access to personal data is password protected. Individual passwords:

- are continually monitored and updated;
- are subject to minimum length requirements;

- are subject to complexity stipulations (e.g. use of certain characters).

Decommissioned IT equipment

8. Decommissioned IT and electrical equipment has data destruction procedures applied as part of its disposal pursuant to the Waste Electrical and Electronic Equipment Regulations 2013 ("WEEE"). All retrievable data thereon is certified as having been safely removed for the purposes of data protection legislation.

Personal devices

9. Personal devices must be configured in accordance with the instructions set out in the IT Acceptable Use Policy for Staff. Any College data that has been copied or replicated to personal devices or systems must be deleted immediately on leaving the College's employment. This includes deleting profiles for College email accounts configured on personal devices.

Transfer of Data to Third Parties

10. The College ensures that prior to the transfer of any personal data to a third party for processing, the third party has appropriate technical and organisational security measures governing the processing to be carried out and has given appropriate contractual assurances for its processing. Any transfers of personal data outside the EU are detailed in the College Record of Data Processing Activities.

Protocol for electronic storage of data

11. This protocol applies to personal data (and other sensitive or confidential) held by the College and its staff electronically. In this protocol, data is classified as follows:

Category	Description	Examples (non-exhaustive)
1	Highly sensitive personal and corporate data which if disclosed could expose the College to financial, legal or safeguarding risk	GDPR sensitive staff/pupil/parent/other individual personal data including health, racial/ethnic origin, religious belief, sexual orientation, biometric data and images of pupils Some sensitive financial data Data Passwords (including complexity recommendations)

2	Confidential personal data	Personal data belonging to staff, parents/guardians, pupils and other users of College facilities and services
3	Sensitive Internal data	College reports, agendas minutes of meetings, financial and legal information waiting lists, pupil reports, generic results and learning support lists
4	Internal data that is not meant for public disclosure.	Teaching materials, team lists, work assignments

12. In order to protect the security and integrity of the various data held by the College, the following principles apply:

- Data which is used for the College's operations must be stored on College provided systems and must not be stored on local hard drives or memory sticks;

- Data which is the property of the College must not be removed or copied from College systems.

13. For ease of reference the storage locations, their security level and categories of data which can be stored on there is set out below:

Storage Location	**Security Level**	**Categories of data which can be stored there**
On Site and Stand Alone Servers (including Virtual Servers and Dedicated Financial Servers) (e.g. ISAMS, DataStore, GP Dynamics (financial), Heritage, (library) and any replacement providers)	High	1 2
Hosted Servers (including Off-Site Hosted Solutions) (e.g. iTrent (HR), Nitrosell, WisePay, Realex, SportsClub, Evolve, Heritage, Survey Monkey, Tapestry, Arbor and any replacement providers)	High	1 2 3

Microsoft Office 365 OneDrive (Preferred Storage location for Staff and Pupils)	Good (User can share data in OneDrive with other College users)	1 (SMT, boarding house masters and those leading College trips only) 2 3 4
On-Site Storage (e.g. My Documents (Staff and Pupil Storage Facility))	Weak	4
USB Attached Storage	Very weak	4

Breach of this Policy

14. The College takes compliance with this policy very seriously. Failure to comply with the policy puts at risk the data subjects whose personal data is being processed, may result in in significant civil sanctions for the College and may amount to a criminal offence by the individual in breach. Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under the College's disciplinary procedures. In the case of a contractor, their contract with the College may be terminated.

Queries

15. If you have any operational queries about this Policy please speak to a member of the Computer Services Department. Legal queries should be referred to Clerk to Governors (legal@dulwich.org.uk).

Policy Owner: Clerk to the Governors
Last Reviewed: January 2023
Date of Next Review: January 2025