DULWICH COLLEGE
FOUNDED 1619

DATA PROTECTION POLICY

Introduction

1. Dulwich College needs to collect, store and process personal data in order to carry out its functions and activities. The College is a data controller for most of the personal data it processes and is committed to full compliance with the applicable data protection legislation (including the UK version of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018)).

2. This Policy sets out the College's expectations and procedures with respect to processing any personal data we collect from data subjects (including parents, pupils, employees, contractors and third parties). All College staff and any other party who handles personal data on behalf of the College are obliged to comply with this Policy when doing so.

3. This Policy also extends to the College's trading subsidiaries, Dulwich College Enterprises Ltd and Dulwich College Enterprises Overseas Ltd and references to "the College" and "we" in this Policy includes those subsidiaries.

4. In this policy:

- "Data processor" refers to an organisation that processes personal data on behalf of the College (as a data controller) for example a payroll or IT provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.

- "Personal data" means any information relating to an identified or identifiable living natural person (referred to as a 'data subject'). An identifier includes unique ID numbers, initials, job titles and nicknames. The information covered by this Policy includes all information created, used or transmitted by or on behalf of the College (including emails and minutes) in whatever media (computer systems, hand-held devices, phones and paper records etc.). The definition of personal information also includes expressions of opinion about an individual or any indication of the College's, or any person's, intentions towards that individual.

- "Processing" is anything done with personal information data, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.

- "Sensitive personal data" (sometimes referred to as" special categories of personal data") are personal data revealing an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.

Data protection principles

5. The College will comply with the following data protection principles when processing personal data:

- we will process personal data lawfully, fairly and in a transparent manner;
- we will collect personal data for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;
- we will only process the personal data that is adequate, relevant and necessary for the relevant purposes;
- we will keep accurate and up to date personal data, and take reasonable steps to ensure that inaccurate personal data are deleted or corrected without delay;
- we will keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed; and
- we will take appropriate technical and organisational measures to ensure that personal data is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

Basis for Processing personal data

6. In relation to any processing activity that involves personal data we will review the purposes of the particular processing activity, and select the most appropriate lawful basis for that processing, i.e.:

- that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- that the processing is necessary for the purposes of the legitimate interests of the College or a third party (except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject);
- that the data subject has consented to the processing;
- that the processing is necessary for compliance with a legal obligation to which the College is subject;
- that the processing is necessary for the protection of the vital interests of the data subject or another natural person (e.g. safeguarding); or
- that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority by the College.

7. Except where the processing is based on consent, we will satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose).

Sensitive personal data

8. The College may from time to time need to process sensitive personal data. We will only process sensitive personal data if we have a lawful basis for doing so (see above) and one of the special conditions for processing sensitive personal data applies, e.g.:

- the data subject has given explicit consent;
- the processing is necessary for the purposes of exercising the employment law rights or obligations of the College or of the data subject;
- the processing is necessary to protect the data subject's vital interests, and the data subject is physically or legally incapable of giving consent;
- the processing relates to personal data which are manifestly made public by the data subject;
- the processing is necessary for the establishment, exercise or defence of legal claims; or
- the processing is necessary for reasons of substantial public interest.

Data privacy impact assessments

9. Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where the College is planning to use a new form of technology), we will, before commencing the processing, carry out a data privacy impact assessment (or DPIA) to assess whether the processing is necessary and proportionate in relation to its purpose, the risks to individuals; and what measures can be put in place to address those risks and protect personal data.

Documentation and records

10. We will keep written records of processing activities and conduct periodic reviews of the personal data we process and update our documentation accordingly.

11. The College will issue privacy notices from time to time, informing people about the personal data that we collect and hold relating to them, how they can expect their personal data to be used and for what purposes. We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Individual rights

12. Data subjects have various rights in relation to their personal data, including the following (subject to various legal exceptions):

- to be informed about how, why and on what basis that data is processed (at the College, we customarily do that via privacy notices);
- to obtain confirmation that their data is being processed and to obtain access to it and certain other information, by making a 'subject access request';
- to have data corrected if it is inaccurate or incomplete; and
- to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten').

13. Individuals are responsible for helping the College keep their personal data up to date and should let the College know if any information they have provided to the College changes.

14. None of the above rights for individuals are unqualified and exceptions may well apply.

Children

15. Children aged 13 and above are generally assumed to have the requisite level of maturity to make decisions about their personal data (e.g. to give consent to processing or to make a subject access request themselves), although this will depend on both the child and the personal data requested, including any relevant circumstances at home. Children younger than 13 may be sufficiently mature.

Information security

16. The College will use appropriate technical and organisational measures to keep personal data secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

17. Where the College uses data processors to process personal data on its behalf, this engagement must be subject to appropriate due diligence and appropriate arrangements need to be implemented in contracts with those organisations to safeguard the security of personal data.

Retention of personal data

18. Personal data (and sensitive personal data) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal data was obtained.

19. Personal data (and sensitive personal data) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

Data breaches

20. A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

21. Examples of a data breach include the following:

- An IT security breach (e.g. the College's systems being hacked into);
- Losing an un-encrypted (i.e. unlocked) laptop, mobile phone, USB stick or a physical file / document containing personal data;
- Sharing confidential pupil/staff matters with individuals who do not need to know it;
- Emails: misdirected / containing the wrong information or information that should not be shared;
- Allowing other members of your household to see confidential documentation you are working on at home;
- Throwing away a document containing the names and addresses of a group of pupils in an ordinary wastepaper bin; and
- Sharing photos without consent (when required).

22. The College will:

- investigate any reported actual or suspected data security breach;
- where applicable, make the required report of a data breach to the Information Commissioner's Office (ICO) without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals;

- notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law; and

- keep a record of any personal breaches, regardless of whether they need to be reported to the ICO.

International transfers

23. The College may transfer personal data outside the European Economic Area[1] to other countries on the basis that such countries are designated as having an adequate level of protection or that the organisation receiving the information has provided adequate safeguards (e.g. by way of binding corporate rules or standard data protection clauses) or where we obtain the relevant data subjects' explicit consent to such transfers. We will inform data subjects of any envisaged international transfers in the relevant privacy notice.

Critical Staff Responsibilities

24. **Record Keeping:** It is important that personal data held by the College is accurate and fair. As such:

- Staff are required to let the College know if the information they have provided to the College changes (for example if they move house or change bank).

- Staff must record the personal data of others – in particular colleagues, pupils and their parents (past, current and prospective) – in a way that is professional and appropriate. Staff should be aware of individuals' rights set out above, whereby any individual about whom they record information on College business (in emails/notes and whether digitally or in hard copy files) may have the right to see that information. This absolutely must not discourage staff from making necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils/parents, in accordance with the College's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position for staff is to record every document or email in a form they would be prepared to stand by should the person about whom it was recorded ask to see it.

25. **Data Handling:** Members of staff (including self-employed contractors and contractors who work for the College via service companies) will have access to the personal data of other members of staff, pupils, alumni, parents, prospective parents/pupils, clients and others in the course of their employment or engagement. The College expects staff to help the College meet its data protection obligations. In particular, staff must:

- only access the personal data that they have authority to access, and only for authorised purposes and must only allow others to access personal data if they have appropriate authorisation to do so;

[1] The EEA comprises the countries in the European Union and Iceland, Liechtenstein and Norway.

- be aware that data security is not simply an online or digital issue but one that effects daily processes e.g. filing and sending correspondence; staff should always consider what they most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access;

- as applicable, liaise with IT and legal as required if they are proposing to use/appoint any new data processors e.g. online apps etc.; and

- handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and in accordance with all relevant College policies and procedures (to the extent applicable to them), particularly the ICT Acceptable Use Policy (Staff) and the Data Security Policy.

26. **Data breaches**: One of the key obligations contained in the GDPR is avoiding, mitigating and reporting personal data breaches. To avoid data breaches staff must:

- Use complex passwords.

- Not open emails/attachments unless clear who it is from.

- Report spam emails/loss of IT equipment containing personal data to IT immediately.

- Only share personal data with those who have a need to know it.

- Check the content of emails carefully and all email addresses before pressing "send" and use "bcc" where addresses of recipients should not be shared.

- Ensure all remote devices are stored securely and password protected.

- Not transfer personal information from previous roles onto College systems.

- Not use personal emails for work.

If a member of staff becomes aware of a personal data breach they **must** notify the Clerk to the Governors at legal@dulwich.org.uk. If in any doubt as to whether to report something internally, it is always best to do so. A personal data breach may be serious, or it may be minor; and it may involve fault or not; but the College always needs to know about them to make a decision.

27. **Subject Access Requests (SARs)**: As stated above, individuals have a right to access their personal data, and such a request must be dealt with promptly:

- A request does not need any formality; an individual can make a SAR verbally or in writing (including by social media) and request does not have to include the phrases 'subject access request'. They can make it to any department in the College, and they do not have to direct it to a specific person or contact point.

- As stated above, children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most requests may not be granted without the express permission of the pupil.

- The College may not always disclose information for a variety of reasons, for example: (i) if it might cause serious harm to the health of the individual; (ii) another person's personal data cannot be anonymised; and (iii) if the disclosure contains sensitive documents relating to crime or legal proceedings or would reveal that a child is being abused.

- If a member of staff becomes aware of a SAR (or is unclear regarding any communication from an individual about their personal data), they must immediately inform the Clerk to the Governors on legal@dulwich.org.uk.

Consequences of failing to comply

28. 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.

Training

29. Staff will receive appropriate training regarding their data protection responsibilities.

Queries

30. If you have any query about this Policy or believe that the College may have breached data protection legislation, please contact the Clerk to Governors, Dulwich College, Dulwich Common, London SE21 7LD. Phone: 0208 299 9306 Email: legal@dulwich.org.uk.

31. Individuals have the right to take any complaints about how the College processes their personal data to the Information Commissioner's Office (ICO), Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF (Tel: 0303 123 1113 Website: www.ico.org.uk/concerns). Please note that the ICO recommends that steps are taken to resolve matters with the relevant organisation before involving the ICO.