GDPR Privacy Notice

Dover College

Owner:	HR	Date: January 2024
Approved By:	CSM	Date: January 2024
Review Frequency	24 Months	
Last reviewed on:	January 2024	
Next review due by:	September 2026	

1. Introduction

Dover College respects your privacy and is committed to protecting your personal data. This privacy notice will inform you as to how we look after your personal data with regards to HR activities. It is for current and former staff of the College, including full-time, part-time, permanent, and self employed employees, independent contractors, consultants and other outsourced and non-permanent workers. It is also relevant for individuals applying for jobs at the College. This policy is intended to provide information about how the school will use (or "process") personal data about individuals including: its staff; its current, past and prospective pupils; and their parents, carers or guardians (referred to in this policy as "parents").

This Privacy Notice applies alongside any other information the school may provide about a particular use of personal data, for example when collecting data via an online or paper form

DATA PROTECTION OFFICER (DPO) VS. DATA
COMPLIANCE OFFICER

Under the GDPR, a data controller will only be required to appoint a DPO if any of the below three conditions are met:

- The processing is carried out by a 'public authority'.
- The 'core activities' require regular and systematic monitoring of data subjects on a 'large scale'.
- Where 'core activities' involve 'large scale' processing of 'special categories' of personal data and relating to criminal convictions and offences.

In the case ofDover College none of these conditions are met, as outlined below, and therefore the school is not required to appoint a DPO.

- As an independent school, Dover College does not qualify as a 'public authority'. This is affirmed by the definitions of 'public authority' and 'public body' given in both the Freedom of Information Act 2000 and the Data Protection Act 2018.
- As an educational provision, the 'core activity' at Dover College is teaching, which does not entail regular and systematic monitoring of data subjects on a 'large scale'.
- Neither the number of data subjects monitored, nor the volume of personal data processed by Dover College qualifies as 'large scale' by a reasonable interpretation of the term,as measurements are not specified in legislation.

In contrast to the statutorily defined role and position of a DPO, Dover College employs a more flexible and equitable approach. All members of the senior leadership team are expected to promote and uphold best practice within the remit of their role and among the staff they oversee. For the purposes of centralising organisational responsibility, the School has appointed the Director of Finance and Operations (DFO) as the Privacy and Compliance Officer (PCO) with responsibility lying with the Head Teacher and the Governors. Ultimately, however, it remains the responsibility of the data controller (the school) to make final decisions about whether to report a breach, disclose or amend a record or agree the terms of a contract with a data processor; the Privacy and Compliance Officer's role is merely to offer advice and guidance.

Like a DPO, the Privacy and Compliance Officer will monitor the organisation's compliance with the GDPR. When deciding whether or not to appoint a DPO, Dover College gave significant consideration to the guidance Data Protection Officers and independent schools': guidance on whether to appoint, published by Farrer & Co through the Independent Schools' Bursars Association in 2020..

1.1 The College takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the Data Protection Act 2018 (the '2018 Act') and

the EU General Data Protection Regulation ('GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

1.2 This policy applies to current and former employees, workers, volunteers, apprentices and consultants. If you fall into one of these categories then you are a 'data subject' for the purposes of this policy. You should read this policy alongside your contract of employment (or contract for services) and any other notice we issue to you from time to time in relation to your data.

1.4 The Company has measures in place to protect the security of your data in accordance with our Data Security Policy. A copy of this can be obtained from HR.

1.5 The College will hold data in accordance with our Data Retention Policy. A copy of this can be obtained from HR We will only hold data for as long as necessary for the purposes for which we collected it.

1.6 The College is a 'data controller' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.

1.7 This policy explains how we will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, the Company.

1.8 This policy does not form part of your contract of employment (or contract for services if relevant) and can be amended by the Company at any time. It is intended that this policy is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this policy, the Company intends to comply with the 2018 Act and the GDPR.

2 Data Protection Principles

Personal data must be processed in accordance with six 'Data Protection Principles.' It must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

We are accountable for these principles and must be able to show that we are compliant.

3 How We Define Personal Data

'Personal data means information which relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

This personal data might be provided to us by you, or someone else (such as a former employer, your doctor, or a credit reference agency), or it could be created by us. It could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. It could be created by your manager or other colleagues.

We will collect and use the following types of personal data about you:

- recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;
- your contact details and date of birth;
- the contact details for your emergency contacts;
- your gender;
- your marital status and family details;
- information about your contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement;
- Your bank details and information in relation to your tax status including your national insurance number;
- your identification documents including passport and driving licence and information in relation to your immigration status and right to work for us;
- information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings);
- information relating to your performance and behaviour at work;
- training records;
- electronic information in relation to your use of IT systems/swipe cards/telephone systems;
- your images (whether captured on CCTV, by photograph or video);
- any other category of personal data which we may notify you of from time to time.

4 How We Define Special Categories of Data

Special categories of personal data are types of personal data consisting of information as to:

- your racial or ethnic origin
- your political opinions
- your religious or philosophical beliefs
- your trade union membership
- your genetic or biometric data
- your health
- your sex life and sexual orientation and
- any criminal convictions and offences.

We may hold and use any of these special categories of your personal data in accordance with the law.

5 Examples of when we might process your personal data

We have to process your personal data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement).

For example:

- to decide whether to employ (or engage) you;
- to decide how much to pay you, and the other terms of your contract with us;

- to check you have the legal right to work for us;
- to carry out the contract between us including where relevant, its termination;
- training you and reviewing your performance;
- to decide whether to promote you;
- to decide whether and how to manage your performance, absence or conduct;
- to carry out a disciplinary or grievance investigation or procedure in relation to you or someone else;
- to determine whether we need to make reasonable adjustments to your workplace or role because of your disability;
- to monitor diversity and equal opportunities;
- to monitor and protect the security (including network security) of the Company, of you, our other staff, customers and others;
- to monitor and protect the health and safety of you, our other staff, customers and third parties;
- to pay you and provide pension and other benefits in accordance with the contract between us;
- paying tax and national insurance;
- to provide a reference upon request from another employer;
- to pay trade union subscriptions;
- monitoring compliance by you, us and others with our policies and our contractual obligations;
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us
- to answer questions from insurers in respect of any insurance policies which relate to you
- the prevention and detection of fraud or other criminal offences;
- to defend the Company in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure

6 Sharing Your Personal Data

Sometimes we might share your personal data with group companies or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests.

We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

We do not send your personal data outside the European Economic Area. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

7 How Should You Process Personal Data at Dover College

Everyone who works for, or on behalf of, the College has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Company's Data Security

The School has appointed the Director of Finance and Operations (DFO) as the Privacy and Compliance Officer. They will deal with all requests and enquiries concerning the School's uses of your personal data (see section on Your Rights below) and endeavour to ensure that all personal data is processed in compliance with this policy and Data Protection Law and updating the Senior Leadership Team and Board of Governors on the College's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person.

You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of the Company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

You should not share personal data informally.

You should keep personal data secure and not share it with unauthorised people.

You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.

You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.

You should use strong passwords.

You should lock your computer screens when not at your desk.

Personal data should be encrypted before being transferred electronically to authorised external contacts. Speak to IT for more information on how to do this.

Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.

Do not save personal data to your own personal computers or other devices.

You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.

You should not take personal data away from Company's premises without authorisation from your line manager or Privacy and Compliance Officer

Personal data should be shredded and disposed of securely when you have finished with it.

You should ask for help from our Privacy and Compliance Officer if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.

It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

8 How to Deal with Data Breaches

We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals then we must also notify the Information Commissioner's Office within 72 hours.

If you are aware of a data breach you must contact Sue Davis, Privacy and Compliance Officer and Wayne Bensted, IT Manager immediately and keep any evidence you have in relation to the breach.

9 Subject Access Requests

You can make a '**subject access request**' ('SAR') to find out the information we hold about you. This request must be made in writing. If you receive such a request you should forward it immediately to the Privacy and Compliance Officer who will coordinate a response.

We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

10 Complaints

You have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

11 Retention of Personal Data

It is important to remember that many of our school records are helpful to keep, not only for former employees and pupils but also for local historical and genealogical research. Following the guidelines set out below ensures that we are compliant with GDPR and the Freedom of Information Act 2000.

File Description	**Data Protection Issue**	**Retention Period**	**Action at end of records life**
Admissions Registers	Yes	Entry + 7 years	Retain in school for 7 years from entry. Can archive these records if needed.
Attendance Registers	Yes	Date of register + 3 years	Are retained whilst the pupils are still at school and for three years after the last date in the register. After it must be securely disposed.

Public Examination results	No	Year of examination +6 years	Secure disposal
Internal Examination results	Yes	Current year +5 years	Secure disposal
Pupil's work	Yes	Current year +1 year	We recommend reviewing these records at the end of each year and allocate a new retention period. Secure disposal.
Timetable	No	Current year +1 year	We recommend reviewing these records at the end of each year and allocate a new retention period. Secure disposal.
Staff timesheets, sick pay	Yes	Current year +6 years	Secure disposal.
Staff personnel files	Yes	Termination +25 years	Secure disposal.
Accessibility plans	Yes	Current year +6 years	Secure disposal.
Incident Reports	Yes	Current year + 20 years	Secure disposal.
School Brochure or prospectus	No	Current year + 3 years	Disposal & recycle.
Annual Accounts		Current year + 6 years	Secure disposal.
Pupil files primary	Yes	Retain for time which the pupil is at the primary school	Transfer the files to their secondary school (or other primary school) when the child leaves.
Pupil files	Yes	Date of birth +25	Secure disposal.

secondary		years	