DATA PROTECTION POLICY

AUTHOR	Data Protection Lead	Date: October 2025
REVIEWED BY	Data Protection and Cyber Security Committee	Date: October 2025
APPROVED BY THE LEADERSHIP TEAM		Date: October 2025
VERSION CONTROL		Version 1

DATE OF NEXT REVIEW	Data Protection Lead	Date: October 2028
REGULATORY COMPLIANCE	Data Protection Act (2018) UK General Data Protection Regulation	
PUBLICATION	Firefly/Atlas, Website	

CONTENTS

Background 2
Definitions 2
Application of this policy 2
Person responsible for Data Protection at the College 3
The Principles 3
Lawful grounds for data processing 4
Headline responsibilities of all staff 4
Rights of Individuals 5
Data of young people 6
Data Security: online and digital 6
Processing of Financial / Credit Card Data 6
Data breach 7
Failure to comply 7
Concerns 7

BACKGROUND

Eton College (the College) is committed to protecting personal data and securing the privacy rights of individuals. During the course of our activities, we collect, store and process personal data, special category data and, occasionally, criminal offence data about staff, pupils, their parents, contractors, donors and other third parties (in a manner more fully detailed in the College's Privacy Notices). Given the nature of the College's work, we recognise that sometimes this data can be sensitive in nature. The College, as the data controller, is responsible for the actions of its staff in how they handle data. It is, therefore, an area where all staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data handling is sensitive or routine.

UK data protection law consists primarily of the UK version of the General Data Protection Regulation (the UK GDPR) and the Data Protection Act 2018 (DPA 2018). The DPA 2018 includes specific provisions of relevance to independent schools: in particular, in the context of our safeguarding obligations, and regarding the right of access to personal data.

The Information Commissioner's Office (ICO) is responsible for enforcing data protection law in the UK and has various powers to take action for breaches of the law.

DEFINITIONS

Key data protection terms used in this data protection policy are:

- **Data Controller** – a person or body that determines the purpose and means of the processing of personal data, and who is responsible for how it is used. For example, the College is a data controller. An independent contractor who makes their own such decisions is also, separately, likely to be a data controller.
- **Data Processor** – an organisation that processes personal data on behalf of a 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 breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- **Personal information or personal data:** any information relating to a living individual (a data subject) by which that individual may be identified by the controller. That is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the College's, or any person's, intentions towards that individual.
- **Processing** – virtually anything done with personal 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.
- **Special categories of personal data –** data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

APPLICATION OF THIS POLICY

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, donors, employees, contractors and third parties).

Those who handle personal data as employees of the College are obliged to comply with this policy when doing so. For employees, a breach of this policy may result in disciplinary action. Accidental breaches of the law or this policy in handling personal data will happen from time to time, for example

by human error, and will not always be treated as a disciplinary issue. However, failure to report breaches that pose significant risks to the College or to individuals will be considered a serious matter.

In addition, this policy represents the standard of compliance expected of those who handle the College's personal data as contractors, whether they are acting as 'processors' on the College's behalf (in which case they will be subject to binding contractual terms) or as controllers responsible for handling such personal data in their own right.

Where the College shares personal data with third parties – which may range from other schools to parents and appropriate authorities – each party will need a lawful basis to process that personal data, and will be expected to do so lawfully and with due regard to security and confidentiality, as set out in this policy.

If you are a volunteer or contractor, you may be a data controller in your own right, but the same legal regime and best practice standards set out in this policy will apply to you by law, and data subjects may contact you directly to exercise their rights.

PERSON RESPONSIBLE FOR DATA PROTECTION AT THE COLLEGE

Matt Brooks acts as the College's Data Protection Lead. He will endeavour to ensure that all personal data is processed in compliance with this policy and the principles of applicable data protection legislation. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to him:

Name: Matt Brooks
Email: Dataprotection@etoncollege.org.uk
Phone: 01753 370542

THE PRINCIPLES

The UK GDPR sets out seven principles relating to the processing of personal data which must be adhered to by controllers (and processors). These require that personal data must be:

1. Processed **lawfully, fairly** and in a **transparent** manner;
2. Collected for **specific and explicit purposes** and only for the purposes it was collected for;
3. **Relevant** and **limited** to what is necessary for the purposes it is processed;
4. **Accurate** and kept **up to date**;
5. **Kept for no longer than is necessary** for the purposes for which it is processed; and
6. Processed in a manner that ensures **appropriate security** of the personal data.
7. The data controller is **accountable** for compliance with the principles of the UK GDPR which includes having the appropriate policies in place.

The UK GDPR's broader 'accountability' principle also requires that the College is able to *demonstrate* that our processing is lawful. This involves, among other things:

- keeping records of our data processing activities, including by way of logs and policies;
- documenting significant decisions and assessments about how we use personal data (including via formal risk assessment documents called Data Protection Impact Assessments (DPIA); and
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were updated; when staff training was undertaken; how and when any data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc.
- maintaining robust assurances to the Provost and Fellows (governors) that data protection procedures are adequate by regularly reviewing the Register of Breaches and performing spot-checks of the compliance framework.

LAWFUL GROUNDS FOR DATA PROCESSING

Under the UK GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, given the relatively high bar of what constitutes consent under the UK GDPR (and the fact that it can be withdrawn by the data subject) it is considered preferable for the College to rely on another lawful ground where possible.

One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the College. It can be challenged by data subjects and also means the College is taking on extra responsibility for considering and protecting people's rights and interests. The College's legitimate interests are set out in its Privacy Notice, as the UK GDPR requires.

Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment, engagement of services and diversity;
- contractual necessity, e.g. to perform a contract with staff or parents, or the engagement of contractors;
- a narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds. In order for us to process 'sensitive data' we are also required to process it in line with the grounds listed in Schedule 2 of the DPA.

HEADLINE RESPONSIBILITIES OF ALL STAFF

Record-keeping

It is important that personal data held by the College is accurate, fair and adequate. Staff are required to inform the College if they believe that *any* personal data is inaccurate or untrue or if the subject is dissatisfied with how it is recorded. This applies to how staff record their own data, and the personal data of others – in particular colleagues, pupils and their parents – in a way that is professional and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information on College business (notably in emails and notes) 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 and 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**.

Data handling

All staff have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and in accordance with this policy and all relevant College policies and procedures (to the extent applicable to them). In particular, there are data protection implications across a number of areas of the College's wider responsibilities such as safeguarding and IT security etc.

The principle of privacy by design is central to the development of all forms of new processing. The creation and generation of new personal data / records, as above, should always be done fairly, lawfully, responsibly and securely.

Avoiding, mitigating and reporting data breaches

Staff need to be adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

One of the key obligations contained in the UK GDPR is on reporting personal data breaches. Controllers must report certain types of personal data breaches (those which risk an impact to individuals) to the ICO within 72 hours. At the College, the Data Protection Lead will determine whether a breach needs to be reported to the ICO, therefore, it is vital that any potential breaches by staff are notified to him immediately.

In addition, controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, the College must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If staff become aware of a personal data breach they must notify Matt Brooks (Data Protection Lead) immediately. If staff are 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.

As stated above, the College may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the College, and for those affected, and could be a serious disciplinary matter whether under this policy or the applicable staff member's contract.

Care and data security

More generally, we require all College staff (and expect all of our contractors) to remain mindful of the data protection principles, and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue but one that effects daily processes: filing and sending correspondence, notably hard copy documents. Data handlers should always consider what their most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

We expect all those with management / leadership responsibilities to be particular champions of these principles and to oversee the swift reporting of any concerns about how personal information is used by the College to Matt Brooks, and to identity the need for (and implement) regular staff training. Staff must attend any training we require them to.

Use of third party platforms / suppliers

As noted above, where a third party is processing personal data on the College's behalf it is likely to be a data 'processor', and this engagement must be subject to appropriate due diligence and contractual arrangements (as required by the UK GDPR). It may also be necessary to complete a DPIA before proceeding – particularly if the platform or software involves any sort of novel or high risk form of processing (including any use of artificial intelligence ("AI") technology). Any request to engage a third party supplier should be referred to Matt Brooks in the first instance, and at as early a stage as possible.

If it is agreed (between yourselves and the Data Protection Lead) that a DPIA is needed (impact assessment of sharing data with a third party) a template form can be found here.

RIGHTS OF INDIVIDUALS

In addition to the College's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a controller (i.e. the College). This is known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation. If you become aware of a subject access request (or indeed any communication

from an individual about their personal data), you must tell Matt Brooks (Data Protection Lead) as soon as possible.

Individuals also have legal rights to:

- require us to correct the personal data we hold about them if it is inaccurate;
- request that we erase their personal data (in certain circumstances);
- request that we restrict our data processing activities (in certain circumstances);
- receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller; and
- object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them.

None of the above rights for individuals are unqualified and exceptions may well apply. However, certain rights are absolute and must be respected, specifically the right to:

- object to automated individual decision-making, including profiling (i.e. where a significant decision is made about the individual without human intervention);
- object to direct marketing; and
- withdraw one's consent where we are relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

In any event, however, if you receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell Matt Brooks (Data Protection Lead) as soon as possible.

DATA OF YOUNG PEOPLE

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.

DATA SECURITY: ONLINE AND DIGITAL

The College must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

No member of staff is permitted to remove personal data from College premises, whether in paper or electronic form and wherever stored, without prior consent from their line manager.

- No member of staff should provide personal data of pupils or parents to third parties, including a volunteer or contractor, unless there is a lawful reason to do so.
- Where a worker is permitted to take data offsite on memory sticks or personal devices it will need to be encrypted.
- Use of personal email accounts or unencrypted personal devices by governors or staff for official College business is not permitted.

PROCESSING OF FINANCIAL / CREDIT CARD DATA

The College complies with the requirements of the PCI Data Security Standard ("PCI DSS"). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. If you are unsure in this regard please seek further guidance from the Bursar. Other categories of financial information, including bank details and salary, or information commonly used in identity theft (such as national insurance numbers or passport details) may not be

treated as legally sensitive, but can have material impact on individuals and should be handled accordingly.

DATA BREACH

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.

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 (sharing the Register of Personal Breaches with the Regulatory and Compliance Committee of the Provost & Fellows biannually).

FAILURE TO COMPLY

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.

CONCERNS

If you have any questions or concerns about anything in this policy, do not hesitate to contact the College's Data Protection Lead (Matt Brooks) at Dataprotection@etoncollege.org.uk or 01753 370542.

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: https://ico.org.uk/make-a-complaint/). Please note that the ICO recommends that steps are taken to resolve matters with the relevant organisation before involving them.