CANBURY SCHOOL

Data Protection Policy

Last Review Date:	**October 2026**
Policy Owner:	**L Anindita-Beckman**
Approved by:	**Chair of Governors**
Next Review Date:	**October 2028**

Data Protection Policy

1. Background

Data protection is an important legal compliance issue for Canbury School. During the course of the School's activities, it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents and guardians, suppliers and other third parties (in a manner more fully detailed in the School's Privacy Notices). 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 is sensitive or routine.

The Data Protection Act 1998 changed on 25 May 2018 with the General Data Protection Regulation (**GDPR**) implementation. This was an EU Regulation that was directly effective in the UK and, following Brexit, was superseded in UK law by the UK General Data Protection Regulation (**UK GDPR**). A new Data Protection Act 2018 has also been passed to deal with certain issues left for national law: this includes specific provisions of relevance to independent schools. In particular, in the context of our safeguarding obligations, the School has a heightened duty to ensure that pupils' personal data is at all times handled responsibly and securely.

Although Brexit resulted in the UK becoming a "third country", in June 2021 the EU Commisssion granted the UK "adequacy status" which has meant that personal data can continue to flow freely from the EEA to the UK.

While these new laws set out useful legal grounds in this area, in most ways, the new laws are strengthening the rights of individuals and placing tougher compliance obligations on organisations, including schools, that handle personal information. The Information Commissioner's Office (**ICO**) is responsible for enforcing data protection law and has powers to take action for breaches of the law.

Those involved in processing personal data are obliged to comply with this policy when doing so. Accidental breaches will happen and may not be a disciplinary issue, but any breach of this policy may result in disciplinary action.

This policy sets out the school's expectations and procedures with respect to processing any personal data we collect from data subjects (e.g., parents, students, and employees).

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

- **Data controller** – an organisation that determines the purpose and means of the processing of personal data. For example, the school controls students' personal information. As a data controller, we are responsible for safeguarding the use of personal data.

- **Data processor** – an organisation that processes personal data on behalf of a data controller, for example, a payroll provider or other supplier of services.
- **Personal data breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to, personal data.
- **Personal information** (or **personal data**): any information relating to a living individual (a data subject), including name, identification number, location or online identifier such as an email address. Note that personal information created in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings) is still personal data and regulated by data protection laws, including the UK GDPR. Note also that it includes expressions of opinion about the individual or any indication of someone's intentions towards that individual.
- **Processing** – virtually anything done with personal information, 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, and genetic or biometric data used to identify an individual. There are also separate rules for processing personal data relating to criminal convictions and offences.

2. Data Protection Lead

The School has appointed the Bursar as the Data Protection Lead, who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of the UK GDPR. Any questions about the operation of this policy or any concerns that the policy still needs to be followed should be referred to the Data Protection Lead in the first instance.

The Principles

The UK GDPR sets out six principles relating to the processing of personal data which must be adhered to by data controllers (and data 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 used 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.

The UK GDPR's 'accountability' principle also requires that the School not only processes personal data in a fair and legal manner but that we are also 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; and
- Generally having an 'audit trail' vis-à-vis data protection and privacy matters, including, for example, when and how our Privacy Notices were updated, how and when data protection consents were collected from individuals, how breaches were dealt with, etc.

3. 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, because the definition of what constitutes consent has been tightened under GDPR (and the fact that the data subject can withdraw it), it is generally preferable 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 Controller. It can be challenged by data subjects and also means the Controller is taking on extra responsibility for considering and protecting people's rights and interests. The School's legitimate interests are set out in its Privacy Policy, as GDPR requires.

Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment and diversity;
- contractual necessity, e.g. to perform a contract with staff or parents;
- 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.

4. Headline responsibilities of all staff

Record-keeping

It is important that personal data held by the School is accurate, fair and adequate. You are required to inform the School if you believe that *your* personal data is inaccurate or untrue or if you are dissatisfied with the information in any way. Similarly, it is vital that the way you record the personal data of others – in particular colleagues, students and their parents – is accurate, professional and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information in emails and notes on School business may have the right to see that information. This absolutely must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or students, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position is to record every document or email in such a way that you would be able to stand by it if the person about whom it was recorded were to see it.

Data handling

The School's lead data handlers are:

- Privacy Officer, responsible for data protection – Bursar
- Student joining, progress and departure data – Registrar
- Marketing and communications – Bursar
- Student education and academic progress – Deputy Head Academic
- Student safeguarding, welfare and pastoral progress – Assistant Head Pastoral
- Student disciplinary data – Assistant Head Pastoral
- Incidents and accidents – Bursar
- Staff data – Bursar
- Alumni - Bursar

All staff have a responsibility to handle the personal data they come into contact with fairly, lawfully, responsibly, and securely in accordance with all relevant school policies and procedures. In particular, there are data protection implications across a number of areas of the School's wider responsibilities, such as safeguarding and IT security, so all staff should read and comply with the following policies:

- Privacy Notices

- Online Safety Policy
- Data Breach Policy
- Safeguarding Policy
- Staff Code of Conduct
- Mobile Phone and Devices Policy
- Student ICT Acceptable Use Procedure
- Taking, Storing and Using Images of Pupils Policy
- Social Media Policy

Responsible processing also extends to creating and generating new personal data/records, as above, which should always be done fairly, lawfully, responsibly and securely.

Avoiding, mitigating and reporting data breaches

One key new obligation in the UK GDPR is reporting personal data breaches. Data controllers must report certain types of personal data breaches (those which risk an impact to individuals) to the ICO within 72 hours.

In addition, data 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 School must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If you become aware of a personal data breach, you must follow the School's Data Breach Policy and notify the Privacy Officer (the Bursar) at privacyofficer@canburyschool.co.uk. If staff are in any doubt as to whether or not you should report something, it is always best to do so. A personal data breach may be severe, or it may be minor, and it may involve fault or not, but the School always needs to know about a breach to make a decision.

As stated above, the School may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the School and for those affected, and could be a serious disciplinary more generally, we require all School staff to remain conscious of the data protection principles (see section 3 above), to attend any training we require them to, 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 affects daily processes: filing and sending correspondence, notably hard copy documents. Staff should always consider what the 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 the School

uses personal information to the Bursar, and to identity the need for (and implement) regular staff training.

5. Rights of Individuals

In addition to the School's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a data controller (i.e. the School). 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 follow the Subject Access Request Policy and tell the Bursar as soon as possible.

Care and data security

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;
- 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, and
- object to automated individual decision-making, including profiling (where a significant decision is made about the individual without human intervention), and to direct marketing, or to withdraw their consent where we are relying on it for processing their personal data.

Except for the final bullet point, none of these rights for individuals are unqualified and exceptions may well apply. 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 the Bursar as soon as possible.

6. Data Security: paper, online and digital

The School 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. As such:

- With the exception of students' work, no staff member is permitted to remove personal data from School premises, whether in paper or electronic form and however stored, without the prior consent of the Head or Bursar.
- Staff must ensure any personal data, including students' work, is stored securely and is not left unattended if not stored securely, whether on or off the School site.
- Use of personal email accounts for official School business is not permitted.
- Use of personal devices without password protection or encryption is not permitted for official School business.
- Staff are not permitted to use memory sticks to store or transfer School-related data to or from school devices without the prior consent of the Head or Bursar.
- Staff must follow a 'clear desk' policy so that no personal data is left unattended on their desks.
- Staff should use **"SENSITIVE/ HIGHLY SENSITIVE"** in the subject line of an email informing the recipient of the nature of the content before it is opened. Staff should only read such emails in private and they should not be read if students/parents/visitors are present.
- Any sensitive email or the opening of My Concern is only to be done at specific times of the day and never when children are present or in the vicinity of the classroom.

7. Summary

It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly.

A good rule of thumb here is to ask yourself questions such as:

- Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?
- Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?
- What would be the consequences of my losing or misdirecting this personal data?

Data protection law is, therefore, best seen not as oppressive red tape or a reason not to do something necessary or important but as a code of valuable and sensible checks and balances to improve how we handle and record personal information and manage our relationships with people. This is an essential part of the School's culture, and all its staff and representatives are expected to adopt this approach.