DATA PROTECTION POLICY

November 2026
To be renewed November 2027

BACKGROUND

Data protection is an important legal compliance issue for Christ Church Cathedral School (the "**School**"). During the course of the School's activities, we collect, store and process Personal Data (sometimes sensitive in nature) about staff, pupils, their parents, contractors and other third parties (in a manner more fully detailed in our Privacy Notice). We, as the data "controller", are liable for the actions of our staff and governors 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.

Data protection law has in recent years strengthened the rights of individuals and placed tougher compliance obligations on organisations including schools that handle personal information. The Information Commissioner's Office ("**ICO**") is responsible for enforcing data protection law in the UK and will typically look into individuals' complaints routinely and without cost and has various powers to take action for breaches of the law.

DEFINITIONS

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

- A **Data Controller** is a person or body that determines the purpose and means of the processing of Personal Data, and who is legally responsible for how it is used. For example, the School is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a controller.
- A **Data Processor** is 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.

- A **Personal Data Breach** is 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** is 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 School's, or any person's, intentions towards that individual.

- **Processing** means 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** include 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 the processing of Personal Data relating to criminal convictions and offences.

APPLICATION OF THIS POLICY

This policy sets out our expectations and procedures with respect to processing any Personal Data we collect from Data Subjects (including parents, pupils, employees, contractors and third parties).

Those who handle Personal Data as employees or governors of the School are obliged to comply with this policy when doing so. For employees, breaches 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 School or individuals will be considered a serious matter.

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

Where we share Personal Data with third party Data Controllers – 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 will 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.

PERSON RESPONSIBLE FOR DATA PROTECTION AT THE SCHOOL

We have appointed the Bursar as the School's Data Protection Lead. In all matters related to data protection, the Bursar reports to the Data Protection Officer of Christ Church in their role as Data Protection Officer ("**DPO**") of Christ Church within the meaning of UK GDPR. The DPO has overall responsibility for ensuring that all Personal Data is processed in compliance with 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 to the Bursar. In the event of a data breach, the Bursar liaises in the first instance with Christ Church's Data Protection Compliance Manager, who is authorised to make mandatory disclosures to the ICO.

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 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 broader 'accountability' principle also requires that we not only process 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 (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.

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 that we 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 School. It can be challenged by data subjects and also means that we are taking on extra responsibility for considering and protecting people's rights and interests. Our 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.

HEADLINE RESPONSIBILITIES OF ALL STAFF

Record-keeping

It is important that Personal Data we hold is accurate, fair and adequate. You are required to inform the School if you believe that any Personal Data is inaccurate or untrue or if you are dissatisfied with

how it is recorded. This applies to how you record your own data, and the Personal Data of others – in particular colleagues, pupils and their parents – in a way that is professional and appropriate.

You should be aware of the rights set out below, whereby any individuals about whom they record information on School 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 you from making necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils and parents, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position is that you record every document or email in a form you would be prepared to stand by should the person about whom it was recorded ask to see it.

Data handling

You have a responsibility to handle the Personal Data which you come into contact with fairly, lawfully, responsibly and securely and in accordance with the Staff Handbook and all relevant School policies and procedures (to the extent applicable to you). 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 you should read and comply with the following policies:

- our School Security policy and CCTV policy;
- our Pupil Behaviour and Discipline, Safeguarding, Anti-Bullying, and Health and Safety Policies, including as to how concerns, low-level concerns or incidents are reported or recorded (both by and about staff);
- our Data Protection Policy;
- our Internet Safety and ICT Policy; and
- Trips policy

Responsible processing also extends to the creation and generation of new Personal Data / records, as above, which should always be done fairly, lawfully, responsibly and securely.

Avoiding, mitigating and reporting data breaches

One of the key obligations contained in the UK GDPR is on reporting Personal Data Breaches. Controllers must report certain types of Personal Data Breach (those which risk an impact to individuals) to the ICO within 72 hours.

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, we 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 notify the Bursar. If you 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 we always need to know about them to make a decision.

As stated above, we 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 matter whether under this policy or the applicable staff member's contract.

Care and data security

More generally, we require you (and expect all our contractors) to remain mindful of the data protection principles, and to use your best efforts to comply with those principles whenever you 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 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 we use personal information to the Bursar, and to identity the need for (and implement) regular staff training. You must attend any training we require you to.

Use of third-party platforms / suppliers

As noted above, where a third party is processing Personal Data on the School'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 the Bursar in the first instance, and at as early a stage as possible.

RIGHTS OF INDIVIDUALS

In addition to 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 tell the Bursar 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 the Bursar as soon as possible.

DATA SECURITY: ONLINE AND DIGITAL

We 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:

- You are not permitted to remove Personal Data from School premises, whether in paper or electronic form and wherever stored, without prior consent of the Head or Bursar.
- You should not provide the Personal Data of pupils or parents to third parties, including a volunteer or contractor, unless there is a lawful reason to do so.

- You may only access Personal Data when you are working offsite by logging on to the School's IT system which will require the use of your username and password and may include two factor authentication.