SHERBORNE SCHOOLS GROUP

Data Protection Policy

Approving body: Executive Committee
Owner: Chief Operating Officer
Author: Policies, Inspection and Strategy Coordinator

Executive Summary

This policy sets out the Group's expectations and procedures with respect to processing any personal data collected from data subjects (including parents[1], pupils, governors and employees). The policy is primarily aimed at staff and determines how, as a matter of good practice and policy, any personal data (covering parents, pupils, governors and colleagues – past, present and prospective) controlled and processed by the Group should be handled by staff. It is separate from, but should be read in conjunction with, the Group Privacy Notice.

Date of Review: Michaelmas 2025
Date of Approval: 22 September 2025
Issue Number: 1
Review Due: Michaelmas 2026

[1] Within this policy, the term 'parent' includes parents, guardians and carers.

Document Number: GRP_DPL_001

Contents

Background

Data protection is an important legal compliance issue for the Sherborne Groups Group[2] ("SSG" or the "Group"). During the course of the Group's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, carers or guardians (referred to in this policy as "parents"), its contractors and other third parties (in a manner more fully detailed in the Group's Privacy Notice). The Group, as data "controller", is liable for the actions of its 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.

United Kingdom (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 Groups 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.

[2] The Sherborne Schools Group includes Sherborne Boys, Sherborne Girls, Sherborne Prep, Hanford Prep and their trading subsidiaries.

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

Definitions

Key data protection terms used in this policy are:

- **Data Controller** – 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 Group is a Data Controller. An independent contractor who makes their own such decisions is also, separately, likely to be a 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 Group'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 Group's expectations and procedures with respect to processing any personal data we collect from data subjects (including parents, pupils, employees, governors, contractors and third parties).

Those who handle personal data as employees (or governors) of the Group 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 Group or individuals will be considered a serious matter.

In addition, this policy represents the standard of compliance expected of those who handle the Group's personal data as contractors, whether they are acting as 'Processors' on the Group'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 Group shares personal data with third party Controllers – which may range from other Groups, 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.

Responsibility for Data Protection within SSG

The Group has designated a Data Protection Lead for each SSG School who will endeavour to ensure that all personal data is processed in compliance with this policy and the principles of applicable data protection legislation. Any question about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the relevant Data Protection Lead.

The relevant School's Data Protection Lead can be contacted using these details:

- Sherborne Boys – Information, Governance and Privacy Compliance Officer penny.baker@sherborne.org
- Sherborne Girls – Operations Bursar kathleen.cook@sherbornegirls.group
- Sherborne Prep – Information, Governance and Privacy Compliance Officer penny.baker@sherborne.org
- Hanford Prep – Operations Manager opsmanager@hanfordprep.group

The Principles

The UK GDPR sets out six 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.

The UK GDPR's broader 'accountability' principle also requires that the Group not only processes personal data in a fair and legal manner but that the Group is also able to demonstrate that its processing of personal data is lawful. This involves, among other things:

- keeping records of data processing activities, including by way of logs and policies;
- documenting significant decisions and assessments about how personal data is used (including via formal risk assessment documents called Data Protection Impact Assessments (DPIAs); and
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how the Group's Privacy Notices 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 for the Group 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 Group. It can be challenged by data subjects and also means the Group is taking on extra responsibility for considering and protecting people's rights and interests. The Group'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.

Headline responsibilities of all staff

Record-keeping

It is important that personal data held by the Group is accurate, fair and adequate. Staff are required to inform the Group if they believe that any personal data is inaccurate or untrue or if they are 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 Group 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 Group'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 all relevant Group policies and procedures (to the extent applicable to them). In particular, there are data protection implications across a number of areas of the Group's wider responsibilities such as safeguarding and IT security, so all staff should read and comply with the policies relating to:

- Safeguarding and child protection
- Online safety/ E-Safety
- Responsible/ Acceptable use of ICT
- Taking, storing and using images of children
- Working from home
- Social Media
- Staff Code of Conduct

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

If staff become aware of a personal data breach they must notify the relevant Data Protection Lead. If staff are in any doubt as to whether to report something internally, it is always best to do so. One of the key obligations contained in the UK GDPR is on reporting personal data breaches. A personal data breach may be serious, or it may be minor; and it may involve fault or not; but the Group always needs to know about them to make a decision. Data 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, the Group must keep a record of any personal data breaches, regardless of whether the ICO needs to be notified.

As stated above, the Group may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the Group, 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, all Group staff (and contractors) are required to remain mindful of the data protection principles (see above), 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. Individuals handling data 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 champion these principles and to oversee the swift reporting of any concerns about how personal information is used by the Group to the relevant Data Protection Lead, and to identity the need for (and implement) regular staff training. Staff must attend any relevant training the Group requires them to.

Use of third-party platforms / suppliers

As noted above, where a third party is processing personal data on the Group'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).

Rights of Individuals

In addition to the Group'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 Group). This is known as the 'subject access right' (or the right to make a 'subject access request'). Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation. When a member of staff is approached by a data subject making a subject access request (or receive communication from an individual about their personal data), they should tell the relevant Data Protection Lead as soon as possible (contact details under "Responsibility for Data Protection within SSG" above).

Individuals also have legal rights to:

- require the Group to correct the personal data held about them if it is inaccurate;
- request that the Group erase their personal data (in certain circumstances);
- request that the Group restricts data processing activities (in certain circumstances);
- receive from the Group the personal data held 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 the Group's particular processing activities where the individual feels this may have 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 their consent where the Group is relying on it for processing their personal data (this right does not affect 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 any member of staff receives a request from an individual who is purporting to exercise one or more of their data protection rights, they must tell the relevant Data Protection Lead as soon as possible.

Data Security: online and digital

The Group 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 Group premises, whether in paper or electronic form and wherever stored, without prior consent of the relevant Head, COO or Director of External Affairs.
- 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. If in doubt, they should consult the Data Protection Lead.
- where a staff member is permitted to take data offsite on memory sticks or personal devices it will need to be encrypted (the use of online storage makes this highly unusual).
- personal email accounts or unencrypted personal devices should not be used by governors/ trustees or staff for official Group business.

Processing of Financial / Credit Card Data

The Group complies with the requirements of the Payment Card Industry 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 Group's Director of Finance or the Chief Operating Officer. 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.

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 fairly, lawfully, securely and responsibly. Further guidelines regarding the practical handling and retention of data are available in the relevant policies relating to Information and Record Management.

A good rule of thumb is to ask 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 a code of useful and sensible checks and balances to improve how handle and record personal information and manage our relationships with people. This is an important part of the Group's culture and all its staff and representatives need to be mindful of it.

Appendix 1: Summary of Changes

- This is the first issue of this policy for the Sherborne Groups Group and supersedes the relevant individual pre-existing policies.