Data Protection Policy

Last revised: October 2026 **Policy Owner:** Bursar
Next Review: October 2027 **Signed:** Ed Currie, Chair of Governors

Associated Policies and Documents

- Health & Safety Policy
- ICT Acceptable Use Agreements – Pupils, Parents & Staff
- Pupil and Parent Privacy Notice
- Staff Privacy Notice
- Safeguarding and Child Protection Policy
- E-Safety Policy
- Complaints Policy

What this Policy is for

This Policy is not to be confused with the Lyndhurst School's Privacy Notices aimed at staff or others, which is a legal requirement under data protection law (and must generally be provided directly to data subjects).

There is a legal difference between a notice (informing individuals how their personal data is used) and a policy, such as this, which seeks to impose obligations and/or standards of good practice on those to whom it applies.

Who does this Policy apply to?

This Policy is primarily aimed at staff: it describes how, as a matter of good practice and policy, any personal data controlled and processed by the Lyndhurst School – including parents, pupils, contractors and colleagues (past, present or prospective) – should be handled in accordance with law and best practice. Where such staff are concerned, this Policy will inevitably therefore have some overlap or interaction with other policies concerning how staff handle data, notably IT: Acceptable Use, Social Media/Use of Images, Retention of Records, and Safeguarding (including record keeping and information sharing).

Legality

UK GDPR does not set out prescriptive requirements for data protection policies. However, it does confer obligations of accountability, data security and staff competence, and to document processing activities generally, that mean a formal policy is strongly to be recommended. In addition, certain grounds for processing personal data (notably safeguarding) under the Data Protection Act 2018 (DPA 2018) specifically require data controllers to have "appropriate policy documents" in place setting out how the controller meets the compliance standard and how long it keeps such personal data.

Background

Data protection is an important legal compliance issue for Lyndhurst School. During the School's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, children, their parents, its contractors and other third parties. The School, as “data controller”, is liable for the actions of its staff, directors 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.

The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) set out how personal data must be handled. Since the UK left the EU, the UK GDPR has applied in place of the EU UK GDPR. 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 Data (Use and Access) Act 2025 has updated this framework, including new rules from 19 June 2026 on how organisations must handle data protection complaints.

Without fundamentally changing the principles of data protection law, and while providing some helpful new grounds for processing certain types of personal data, in most ways this new law has 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, will typically investigate 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:

- **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 School (including by its directors) is a 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 data 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 school's, or any person'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, 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

This policy sets out the School's expectations and procedures with respect to processing any personal data we collect from data subjects (including parents, children, employees, contractors and third parties).

Those who handle personal data as employees or directors 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 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 the School shares personal data with third party data controllers – which may range from other schools, to parents, to appropriate authorities, to casual workers and volunteers – 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.

Volunteers and contractors who handle personal data on the School's behalf must follow this policy in the same way as staff.

Person responsible for Data Protection at the School

The School has appointed Katie Price, Deputy DSL and member of the Senior Leadership Team, as its Data Protection Lead. She 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 it has not been followed, should be referred in the first instance to the Data Protection Lead.

Raising a Data Protection Concern or Complaint

mailto:dsl@lyndhurstschool.co.ukIf you wish to raise a concern or make a complaint about how your personal data has been handled, please contact Katie Price, the School's Data Protection Lead. You may use the School's Data Protection Complaint Form, which can be requested from her.

This form will collect your personal data, such as your name and contact details, as well as the details of your complaint. This information will be used to process your complaint and respond to you.

mailto:dsl@lyndhurstschool.co.ukmailto:slt@lyndhurstschool.co.ukCompleted forms should be sent to Katie Price, Data Protection Lead, who will investigate the matter in line with the School's procedures.

Complaints made in any other way, including by email or in person, will also be accepted. In line with the Data (Use and Access) Act 2025, the School will:

- acknowledge the complaint within 30 days of receiving it;
- investigate it without undue delay, in a way that is proportionate to the issues raised;
- keep the person informed of progress; and
- tell them the outcome without undue delay.

Complaints are recorded, together with the outcome and any action taken. Anyone who is unhappy with the School's response can complain to the Information Commissioner's Office (ICO) at ico.org.uk or on 0303 123 1113.

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 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 (including via formal risk assessment documents called Data Protection Impact Assessments); 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, because the definition of what constitutes consent has been tightened under UK GDPR (and the fact that it can be withdrawn by the data subject) it is considered preferable for the School 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 School. It can be challenged by data subjects and also means the School 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 Notice, as 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.

Data protection law is not a barrier to sharing information where this is needed to keep a child safe. In line with KCSIE 2026, staff must never delay passing on a safeguarding concern because of data protection worries. The DPA 2018 allows the School to share information, including special category data, without consent where

this is necessary to safeguard a child. Safeguarding records are handled as set out in the Safeguarding and Child Protection Policy.

Headline responsibilities of all staff

Record-keeping

It is important that personal data held by the School is accurate, fair and adequate. Staff are required to inform the School if they believe that any personal data is inaccurate or untrue or if you are dissatisfied with how it is recorded. This applies to how staff record their own data, and the personal data of others – colleagues, children 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 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 staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils, in accordance with the School'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 encounter fairly, lawfully, responsibly and securely and in accordance with the staff handbook and all relevant School policies and procedures (to the extent applicable to them). There are data protection implications across several areas of the School's wider responsibilities such as safeguarding and IT security, so all staff should read and comply with the following policies:

E-Safety Policy, Acceptable Use Agreements, Safeguarding and Child Protection 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 under the UK GDPR is reporting personal data breaches. Data controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours of becoming aware of the breach.

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 staff become aware of a personal data breach they must notify the 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 School always needs to know about them to decide.

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 matter whether under this policy or the applicable staff member's contract.

Care and data security

More generally, we require all School staff (and expect all our contractors) to remain mindful of the data protection principles (see 'The Principles' 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 affects 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 champions of these principles and to oversee the swift reporting of any concerns about how personal information is used by the School to the Data Protection Lead, and to identify the need for (and implement) regular staff training. Staff must attend any training we require them to.

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 tell the Data Protection Lead as soon as possible.

Subject access requests must normally be answered within one month, which can be extended by up to two further months for complex requests. The School will carry out reasonable and proportionate searches for the information requested. Pupils can make their own requests if they are mature enough to understand their rights (usually from around the age of 12); otherwise a parent may make a request on their behalf.

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 situation, to any of our processing activities where the individual feels this has a disproportionate impact on them; and
- complain to the School, and to the ICO, about how their personal data has been handled;

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 Data Protection Lead as soon as possible.

Data Security: 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.

- no member of staff is permitted to remove personal data from School premises, whether in paper or electronic form and wherever stored, without prior consent of the Headmistress or Bursar.
- 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, directors or staff for official School business is not permitted.
- Staff must not enter personal data about pupils, parents or colleagues into AI tools that the School has not approved.

Processing of Financial / Credit Card Data

The School 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.

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