



LOCHINVER
HOUSE

Data Protection Policy

Lochinver House School takes the security and privacy of data seriously and aims to ensure that all personal data collected from employees, pupils, parents, governors, visitors and other individuals (the School Community) is collected, stored and processed in accordance and compliance with the [General Data Protection Regulation \(GDPR\)](#) and the provisions of the Data Protection Act 2018 (DPA 2018) as set out in the [Data Protection Bill](#). The School, 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 the School complies with, and are mindful of, the 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.

This policy applies to all personal data (regardless of whether it is in paper or electronic format) and applies to current and former paid employees, pupils, parents/carers, volunteers, governors and contractors in regulated activity. ‘Data subjects’ are those falling into one of the aforementioned categories for the purposes of this policy.

This policy does not form part of any contract with the School and can be amended by Lochinver House School at any time.

This policy sets out the School’s expectations and procedures with respect to processing any personal data collected 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 ‘processors’ on the School’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 School shares personal data with third party 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.

Person responsible for Data Protection at Lochinver House School

The Data Protection Lead (“DPL”) is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines where applicable. The DPL is also responsible for updating the Governing Body about data protection responsibilities and any risks in relation to the processing of data and is contactable via email at data@lochinverhouse.com. The DPL endeavours 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 the DPL. Staff will receive regular training and updates regarding Data Protection.

Data Protection 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:

- processed fairly, lawfully and in a transparent manner
- collected for specific and explicit purposes and only for the purpose it was collected for
- relevant and limited to what is necessary for the purposes it is processed
- accurate and kept up to date.
- kept for no longer than is necessary for the purposes for which it is processed
- 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 also demonstrates processing is lawful. This involves, among other things:

- keeping records of data processing activities, including by way of logs and policies
- 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 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. The School's legitimate interests are set out in its Privacy Notice. 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.

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 any personal data is inaccurate or untrue or 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 information is recorded on School business (notably in emails and notes) digitally or in hard copy files may have the right to see that information. This 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 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 they come into contact with fairly, lawfully, responsibly and securely and 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 all relevant School policies.

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 its governors) 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.

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.

A personal data breach means 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. It also means that a breach is more than just about losing personal data. In the unlikely event of a suspected data breach, we will follow the procedure set out in guidance on personal data breaches produced by the ICO.

Controllers must notify individuals affected in a data breach if it is likely to result in a "high risk" to their rights and freedoms. 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 DPL. 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 make a decision. Failure to report a potential data breach 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 staff member's contract.

The School has robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) the DPL will take notes and keep evidence of that breach. In the event of becoming aware of a data breach, contact the DPL immediately and secure any evidence in relation to the breach.

Care and Data Security

More generally, we require all members of the School community 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 effects daily processes and data handlers should always consider what they most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

The School ensures that appropriate measures are taken against unlawful or unauthorised processing of personal data and against loss of, or damage to, personal data.

Use of Third Party Platforms / Suppliers

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 DPL in the first instance, and at as early a stage as possible.

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 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 DPL 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 DPL as soon as possible.

Training

All staff receive regular training and updates on data protection.

Policy Reviewed:	01.01.2025
Policy Review Date:	31.12.2026
Policy linked to:	Acceptable Use Policy, Admissions and Attendance Policy, Anti-Bullying Strategy, Assessment and Recording Policy, Behaviour Policy, Biometrics Policy, Bursary Policy, Child Protection and Safeguarding Policy and Procedures (incorporating Staff Behaviour and Code of Conduct), Children Missing from Education Policy, Complaints Policy, Critical Incident Management Plan, Data Retention Policy, Driver's Declaration, Disciplinary, Grievance and Capability Policy, Educational Visits Policy, English as an Additional Language (EAL) Policy, Equal Opportunities Policy, EYFS Supervision, First Aid Policy, Health and Safety Policy, Historical Abuse Policy, Keeping Children Safe in Education (Sept 2022), Marking and Feedback Policy, More Able Policy, Pay Policy, Privacy Notice, Professional Development Policy, Personal, Social, Health and Education (PSHE) Policy, Recruitment Policy, Reports and References Policy, SEND Policy, Spiritual, Moral, Social and Cultural (SMSC) Policy, Supervision Policy, Terms and Conditions, Visitor and Visiting Speaker Policy and Procedure, Whistleblowing Policy.