



# Data Protection Policy

*This school is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment*

<b>Governor's Committee Responsibility:</b>	<b>Resources</b>
<b>Date Approved:</b>	<b>8<sup>th</sup> June 2018</b>
<b>Review Period:</b>	<b>3 yearly</b>
<b>Next Review Date:</b>	<b>Summer 2021</b>

## **The Limpsfield Grange Values:**

At Limpsfield Grange we believe in working together to make a difference.

We are a tolerant community; we accept, value and understand others.

We care for all members of our community without judgement.

We are responsible for our own learning, behaviour and actions.

We accept that sometimes things go wrong. We work together to take responsibility for our mistakes and for putting things right.

We are a respectful community and we treat others as we would like to be treated, even if they have different views and opinions to our own.

We understand that good behaviour helps us to prepare for life beyond Limpsfield Grange.

We are positive and resilient. We celebrate difference in everything that we do.

We are all proud to be part of the Limpsfield Grange community.

*July 2017*

## Limpsfield Grange School – Data Protection Policy

### **Background and rationale**

The General Data Protection Regulation (GDPR) (2018) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

Limpsfield Grange School will protect and maintain a balance between data protection rights in accordance with the GDPR. This policy sets out how we handle the personal data of our students, parents, suppliers, employees, workers and other third parties.

Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

### **Aims of the policy**

To ensure that all data is processed in line with the General Data Protection Regulations 2018.

### **Scope of the policy**

This policy applies to all data created, received or maintained by staff at the school in the course of carrying out its functions. This policy applies to all staff and Governors of Limpsfield Grange, including members of our Outreach Service, and professionals working with students or staff at Limpsfield Grange and professionals who have been commissioned by the school with a service.

### **Definitions**

#### **Personal data**

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for examples a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

### **Special category data**

Previously termed “Sensitive Personal Data”, Special Category Data is similar by definition and refers to data concerning an individual Data Subject’s racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

### **Data subject**

An individual about whom such information is stored is known as the Data Subject. It includes but is not limited to employees.

### **Data controller**

The organisation storing and controlling such information (i.e. the School) is referred to as the Data Controller.

### **Processing**

Processing data involves any activity that includes the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

### **Automated processing**

Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

An example of automated processing includes profiling and automated decision making. Automatic decision making is when a decision is made which is based solely on automated processing which produces legal effects or significantly affects an individual. Automated decision making is prohibited except in exceptional circumstances.

### **Data Protection Impact Assessment (DPIA)**

DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

### **Criminal records information**

This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

### **When can the school process personal data?**

#### **Data protection principles**

Limpsfield Grange is responsible for adhering to the principles relating to the processing of personal data as set out in the GDPR.

The principles which Limpsfield Grange must adhere to are:

- Personal data must be processed lawfully, fairly and in a transparent manner
- Personal data must be collected only for specified, explicit and legitimate purposes
- Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
- Personal data must be accurate and, where necessary, kept up to date

- Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed
- Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage

**Principle 1: Personal data must be processed lawfully, fairly and in a transparent manner**

Limpsfield Grange School only collects, processes and shares personal data fairly and lawfully and for specified purposes. The School must have a specified purpose for processing personal data and special category of data as set out in the GDPR.

Before the processing starts for the first time Limpsfield Grange will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. We will then regularly review those purposes whilst processing continues in order to satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose).

**Personal Data**

Limpsfield Grange may only process a data subject’s personal data if one of the following fair processing conditions are met:

- The data subject has given their consent
- The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract
- To protect the data subject’s vital interests
- To meet our legal compliance obligations (other than a contractual obligation)
- To perform a task in the public interest or in order to carry out official functions as authorised by law
- For the purposes of the School’s legitimate interests where authorised in accordance with data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the data subject.

**Special Category Data**

Limpsfield Grange may only process special category data if they are entitled to process personal data (using one of the fair processing conditions above) AND one of the following conditions are met:

- The data subject has given their explicit consent
- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the School in the field of employment law, social security law or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay
- To protect the data subject’s vital interests
- To meet our legal compliance obligations (other than a contractual obligation)
- Where the data has been made public by the data subject
- To perform a task in the substantial public interest or in order to carry out official functions as authorised by law

- Where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
- Where it is necessary for reasons of public interest in the area of public health
- The processing is necessary for archiving, statistical or research purposes

Limpsfield Grange identifies and documents the legal grounds being relied upon for each processing activity.

### **Consent**

Where Limpsfield Grange relies on consent as a fair condition for processing (as set out above), it will adhere to the requirements set out in the GDPR.

Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. Explicit consent requires a very clear and specific statement to be relied upon (i.e. more than just mere action is required).

A data subject will have consented to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

If explicit consent is required, the School will normally seek another legal basis to process that data. However if explicit consent is required the data subject will be provided with full information in order to provide it.

Limpsfield Grange will keep records of consents obtained in order to demonstrate compliance with consent requirements under the GDPR.

### **Principle 2: Personal data must be collected only for specified, explicit and legitimate purposes**

Personal data will not be processed in any manner that is incompatible with the legitimate purposes.

Limpsfield Grange will not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the data subject of the new purpose (and they have consented where necessary).

### **Principle 3: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed**

Limpsfield Grange will only process personal data when our obligations and duties require us to. We will not collect excessive data and ensure any personal data collected is adequate and relevant for the intended purposes.

When personal data is no longer needed for specified purposes, Limpsfield Grange shall delete or anonymise the data. [Please refer to the School's Data Retention Policy for further guidance].

**Principle 4: Personal data must be accurate and, where necessary, kept up to date**

Limpsfield Grange will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data.

Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant.

Data subjects have the right to request rectification to incomplete or inaccurate data held by the School.

**Principle 5: Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed**

Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. We will ensure that we adhere to legal timeframes for retaining data.

We will take reasonable steps to destroy or erase from our systems all personal data that we no longer require. We will also ensure that data subjects are informed of the period for which data is stored and how that period is determined in our privacy notices.

Please refer to the Limpsfield Grange Retention Policy for further details about how we retain and remove data.

**Principle 6: Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage**

In order to assure the protection of all data being processed, the School will develop, implement and maintain reasonable safeguard and security measures. This includes using measures such as:

- Encryption;
- Ensuring authorised access (i.e. that only people who have a need to know the personal data are authorised to access it)
- Adhering to confidentiality principles
- Ensuring personal data is accurate and suitable for the process for which it is processed

Limpsfield Grange will follow procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data.

Limpsfield Grange will only transfer personal data to third party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place.

**Sharing personal data**

Limpsfield Grange will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. These include if the third party:

- Has a need to know the information for the purposes of providing the contracted services
- Sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained
- The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place
- The transfer complies with any applicable cross border transfer restrictions

- A fully executed written contract that contains GDPR approved third party clauses has been obtained.

There may be circumstances where Limpsfield Grange is required either by law or in the best interests of our students, parents or staff to pass information onto external authorities, for example, the Local Authority, Ofsted or the department of health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of Limpsfield Grange shall be clearly defined within written notifications and details and basis for sharing that data given.

### **Transfer of data outside the European Economic Area (EEA)**

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined.

Limpsfield Grange will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the GDPR. All staff must comply with the School's guidelines on transferring data outside of the EEA. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

### **Data subject's rights and requests**

Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data.

The rights data subjects have in relation to how Limpsfield Grange handles their personal data are set out below:

- (Where consent is relied upon as a condition of processing) to withdraw consent to processing at any time
- Receive certain information about the School's processing activities
- Request access to their personal data that we hold
- Prevent our use of their personal data for marketing purposes
- Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data
- Restrict processing in specific circumstances
- Challenge processing which has been justified on the basis of our legitimate interests or in the public interest
- Request a copy of an agreement under which personal data is transferred outside of the EEA
- Object to decisions based solely on automated processing
- Prevent processing that is likely to cause damage or distress to the data subject or anyone else
- Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms
- Make a complaint to the supervisory authority

- In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format

If any request is made to exercise the rights above, it is a requirement for the relevant staff member within the School to verify the identity of the individual making the request.

### **Data Subject Access Requests**

A Data Subject has the right to be informed by the School of the following:

- Confirmation that their data is being processed
- Access to their personal data
- A description of the information that is being processed
- The purpose for which the information is being processed
- The recipients/class of recipients to whom that information is or may be disclosed
- Details of the School's sources of information obtained
- In relation to any Personal Data processed for the purposes of evaluating matters in relation to the Data Subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct.
- Other supplementary information

Any Data Subject who wishes to obtain the above information must notify the School in writing of his or her request. This is known as a Data Subject Access Request.

The request should in the first instance be sent to the School Business Manager.

### **Direct marketing**

Limpsfield Grange is subject to certain rules and privacy laws when marketing. For example a data subject's prior consent will be required for electronic direct marketing (for example, by email, text or automated calls).

Limpsfield Grange will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand. The School will promptly respond to any individual objection to direct marketing.

### **Employee obligations**

Employees may have access to the personal data of other members of staff, suppliers, parents or students of the School in the course of their employment or engagement. If so, the School expects those employees to help meet the School's data protection obligations to those individuals. Specifically, you must: -

- Only access the personal data that you have authority to access, and only for authorised purposes
- Only allow others to access personal data if they have appropriate authorisation
- Keep personal data secure for example by complying with rules on access to school premises, computer access, password protection and secure file storage and destruction. Not to remove personal data or devices containing personal data from the School premises unless appropriate security measures are in place (such as encryption, password protection) to secure the information
- Not to store personal information on local drives.

## **Accountability**

Limpsfield Grange will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. We are responsible for and demonstrate accountability with the GDPR principles.

The School have taken the following steps to ensure and document GDPR compliance:

### **Data Protection Officer (DPO)**

Please find below details of the School's Data Protection Officer:

Data Protection Officer: Craig Stilwell

Address: Judicium Consulting Ltd, 72 Cannon Street, London, EC4N 6AE

Email: [dataservices@judicium.com](mailto:dataservices@judicium.com)

Telephone: 0203 326 9174

The Data Protection Officer is responsible for overseeing this Data Protection policy and developing data-related policies and guidelines.

Please contact the Data Protection Officer with any questions about the operation of this Data Protection policy or the GDPR or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact the Data Protection Officer in the following circumstances:

- If you are unsure of the lawful basis being relied on by the School to process personal data
- If you need to rely on consent as a fair reason for processing (please see below the section on consent for further detail)
- If you need to draft privacy notices or fair processing notices
- If you are unsure about the retention periods for the personal data being processed [but would refer you to the School's data retention policy in the first instance]
- If you are unsure about what security measures need to be put in place to protect personal data
- If there has been a personal data breach [and would refer you to the procedure set out in the School's breach notification policy]
- If you are unsure on what basis to transfer personal data outside the EEA
- If you need any assistance dealing with any rights invoked by a data subject
- Whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if you plan to use personal data for purposes other than what it was collected for
- If you plan to undertake any activities involving automated processing or automated decision making
- If you need help complying with applicable law when carrying out direct marketing activities
- If you need help with any contracts or other areas in relation to sharing personal data with third parties

### **Personal data breaches**

The GDPR requires Limpsfield Grange to notify any applicable personal data breach to the Information Commissioner's Office (ICO).

We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person designated as the key point of contact for personal data breaches either School Business Manager, or your Data Protection Officer.

### **Transparency and privacy notices**

Limpsfield Grange will provide detailed, specific information to data subjects. This information will be provided through the School's privacy notices which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them. Privacy notices sets out information for data subjects about how Limpsfield Grange use their data and the School's privacy notices are tailored to suit the data subject.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the GDPR including the identity of the Data Protection Officer, the School's contact details, how and why we will use, process, disclose, protect and retain personal data.

When personal data is collected indirectly (for example from a third party or publically available source), we will provide the data subject with the above information as soon as possible after receiving the data. The School will also confirm whether that third party has collected and processed data in accordance with the GDPR.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as "children" under the GDPR

### **Privacy by design**

Limpsfield Grange will adopt a privacy by design approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner.

Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, Limpsfield Grange takes into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data processes.

### **Data Protection Impact Assessments (DPIAs)**

In order to achieve a privacy by design approach, Limpsfield Grange will conduct DPIAs for any new technologies or programmes being used by the School which could affect the processing of personal data. In any event the School carries out DPIAs when required by the GDPR in the following circumstances:

- For the use of new technologies (programs, systems or processes) or changing technologies
- For the use of automated processing
- For large scale processing of special category data
- For large scale, systematic monitoring of a publicly accessible area (through the use of CCTV)

Our DPIAs contain:

- A description of the processing, its purposes and any legitimate interests used
- An assessment of the necessity and proportionality of the processing in relation to its purpose
- An assessment of the risk to individuals
- The risk mitigation measures in place and demonstration of compliance
-

## **Record Keeping**

Limpsfield Grange are required to keep full and accurate records of our data processing activities. These records include:

- The name and contact details of the School
- The name and contact details of the Data Protection Officer
- Descriptions of the types of personal data used
- Description of the data subjects
- Details of the School's processing activities and purposes
- Details of any third party recipients of the personal data
- Where personal data is stored
- Retention periods
- Security measures in place

## **Data security**

Employees should keep all data secure, by taking sensible precautions and following the guidelines below:

- Strong passwords must be used and they should never be shared
- Personal data should not be disclosed to unauthorised people, either within the school community or externally
- Data should be regularly reviewed and updated as necessary
- Personal security codes must be used when printing sensitive data to the photocopiers

## **Data storage**

All data must be stored securely to prevent unauthorised access.

- Paper copies of personal or sensitive information must be stored in a secure place such as a locked drawer or filing cabinet.
- Staff must ensure that papers and printouts are not left where unauthorised people could see them, e.g. on a printer
- Data printouts must be shredded or put into confidential waste bags when no longer required.
- Where data is stored electronically it must be protected from unauthorised access, accidental deletion and malicious hacking attempts.
- Data should be protected by strong passwords that are changed regularly.
- If data is stored on removable media (flashdrive, CD) these should be kept locked away securely when not being used.
- Encrypted, password protected flash drives must be used for any personal or sensitive information being taken off school devices.
- Data should only be stored on designated drives and servers.
- Data should be backed up frequently – both servers are backed up daily.
- Data should never be saved directly onto laptops or other mobile devices such as tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

## **Data use**

- When working on school computers staff should ensure that the screens of their computers are always locked when left unattended.
- Personal data should only be emailed using a secure service such as Egress

- Data must be encrypted before being transferred electronically.

**Training**

Limpsfield Grange will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws.

**Audit**

Limpsfield Grange through its Data Protection Officer will regularly test data systems and processes in order to assess compliance. These are done through data audits which take place annually in order to review use of personal data.

**Related Policies**

Staff should refer to the following policies that are related to this data protection policy:

- Data Retention policy;
- Data Breach policy;
- Security policy
- Safeguarding policy

These policies are also designed to protect personal data and can be found on the school website.

**Monitoring**

This policy will be monitored by the Resources committee of the Governing Body who will receive updates regarding data protection from the School Business Manager and the Headteacher.

The School Business Manager is Sandra Thornhill.

**Links**

<https://ico.org.uk/for-organisations/education/>

**Review**

The Governing Body of Limpsfield Grange School adopted this policy on:

It will be reviewed on:

---

Signed

---

Dated

---

---