# Spring Lane School

# GDPR
# DATA PROTECTION POLICY
# 2022-2023

| | |
|---|---|
| **Document Owner:** | Denise Robinson |
| **Document Type:** | Strategy/Policy/Procedure |
| **Date:** | Jan 2023 |
| **Version:** | V1 |
| **Review Period:** | Annually |
| **Date Approved:** | Nov 2022 |
| **Approved by:** | V Shaw |

| **Version Control Tracking** | | | | |
|---|---|---|---|---|
| **Version** | **Date** | **Revision Description** | **Editor** | **Status** |
| V1 | Nov 21 | Policy creation and updated GDPR rep | DR | approved |
| V1.1 | Nov 22 | Annual Review | DR | Approved |
| V1.1 | Nov 23 | Annual Review | DR | Approved |

**Spring Lane School**
**General Data Protection Regulation**
***Data Protection Policy***

**Spring Lane School Mission Statement**
**'Grow, aspire and achieve'**

## Introduction

Spring Lane School will comply with the demands of the General Data Protection Regulation (GDPR) to be known as the Data Protection Act 2018.

Members of staff will gain familiarisation with the requirements of the GDPR either in a staff briefing or as part of their induction.

This policy follows guidance issued by the Information Commissioner's Office (ICO) and the Department for Education (DfE).

The school is a Data Controller as data is processed that is the personal information of pupils, families, staff, visitors and other school users.

The School is a Data Processor as it processes data on behalf of other public bodies such as the DfE.

## Definitions

*Data processing*
The acquisition, storage, processing and transmission of data

*Data subject*
Any identifiable person whose data is processed

*Consent*
Must be freely given, specific and an unambiguous indication of the subject's wishes. It must be recorded and available to an audit. A person must be 13 years old in order to record their consent.

*Cross-border processing*
The GDPR covers all EU states and will remain part of UK law. Data cannot be stored beyond the EU and UK borders (the exact borders are those of the European Economic Area)

*Sensitive data*
The GDPR/ICO requires that particular care is taken with the following data

- Data regarding children
- Health (physical, mental, genetic)
- Ethnicity
- Religion
- Sexuality
- Performance management and trade union membership

*Filing system*
Any structured set of personal data, however stored in any format (physical or digital) that can be processed

*Personal data breach*
A breach of data security leading to the accidental or unlawful destruction, loss, theft, alteration, unauthorised disclosure, destruction, sale or access to any processed data. Data subjects affected by a data breach must be informed of the breach within 72 hours. Breaches must be reported to the ICO within 72 hours.

*Pseudonymisation*
The act of making data anonymous. There must be security between pseudonymised data and any data that could re-identify a person.

*Password protection*
The act of 'locking' a device or document. The information remains readable beyond the password.

*Encryption*
The act of encoding all the information beyond a password or code.

*Legal basis*
The school decides, and registers with the ICO, upon which legal basis it processes data. As a public body with set duties the school uses the following bases for processing and controlling data

Legal basis: **Public Task**

- Admissions
- Attendance
- Assessment
- Pupil and staff welfare
- Safe recruitment
- Staff training
- Performance Management

Legal basis: **Consent**

- Various uses of photographs and moving images
- Trade union membership
- Staff ethnicity, religion and health data (Note the Staff Privacy Statement)
- The use of data to promote the social life of the school community

Legal basis: **Contract**

- When processing is required to carry out the performance of a contract

*Personal data*
Anything that might lead to the identification of a person: name, number, characteristics, photograph, correspondence.

*Data portability, data subject access request*
Data subjects (or a child's parents) may request access to a copy of all their data. The school has established an efficient means of accomplishing this task which may not carry a charge and will be completed within 15 working days. Data subjects may request that data is brought up-to-date or made more accurate.[1]

## Principles

- Personal data must be processed lawfully, fairly and transparently
- Personal data can only be collected for specific, explicit and legitimate purposes
- Personal data must be adequate, relevant and limited to what is necessary for processing
- Personal data must be accurate and kept up-to-date
- Personal data may identify the data subject only as long as is necessary for processing
- Personal data must be processed in a manner that ensures its security
- Any breaches in data security must be reported to the ICO within 72 hours
- The school must report any breaches caused by third parties who have access to school users' data within 72 hours.
- The school must inform any data subject (person identified in data) where a data breach may have led to the unauthorised access to their personal information [2]

## Roles and Responsibilities

The school's Privacy Statements set out in detail how the school will maintain the security of school users' data. The Acceptable Use Policies set out the duties of the staff and other school users in supporting data security.

The school is a **Data Controller** as we are responsible for decisions about how and why we use your personal information.

At times the school acts as a **Data Processor** when we are required to obtain, process and transfer data on the behalf of external organisations.

The school has appointed a **Data Protection Officer**

Ben Cain

SAMPeople, First floor, Unit A Cedar Court Office Park Denby Dale Road, Wakefield WF4 3FU

Telephone – 01924 907319

Usually the school will coordinate data protection practice through

Denise Robinson – School Business Manager

The governor with special responsibility for data security is Ian Chambers

Ben Cain or SAMPeople may be contacted directly should any employee or contractor feel that their concerns about data protection are not being addressed within the school. Among the DPO's duties are:

- Advice on the secure storage and transmission of data (both physical and digital)
- Updates for the school on the GDPR
- The completion of a data audit
- Support for a data processing record system
- The provision of template GDPR documentation (please note that this cannot be shared beyond the school without the permission of Safeguarding Monitor)

- Reporting to the school's leadership and governing body on levels of security and compliance
- Support with securing certification that they are also complying fully with GDPR duties from third parties who might hold personal data through the school
- The DPO will communicate with the Information Commissioner's Office should there be a confirmed or suspected data breach
- The DPO will communicate with any person whose data might have been improperly accessed, deleted, lost or stolen

The DPO will liaise between the school and the ICO and must be informed as soon as is practicable of any personal data security breach.

The DPO will support the school in its communication with schools users (pupils, families, parents, governors, contractors and visitors) about the school's GDPR procedures. This will include the drafting of privacy statements, acceptable use policies and data subjects rights.

Data subject requests should be made in writing to the DPO. The DPO might have to respond to any or all of the following

- Why the data a is processed
- On which basis
- Who has seen it
- How long it will be stored for
- Where the data was sourced
- Whether decisions have been based on the data

Children below the age of 13 do not have the right to make a subject access request, so requests must be made by parents. The school may take into account the views of a pupil.

## Data Audit

The school will carry out a data audit with support from SAMPeople and their technical support company. Within the audit the school will record all third parties' compliance with the GDPR if those third parties process data for any school users. Such confirmation will, from now on, be an essential part of any contract with third parties when the processing of school users' data is involved. The school will not share data, or have any data processed, by any third parties who do not confirm their compliance with GDPR requirements.

Preferably companies that process school users' data will have certification to ISO27001.

The audit will also check the security of physical and digital records and devices.

## Processing Records

To meet the ICO's recommendation that 'scrupulous records' are developed the school will record its processing of data and the results of its data audit. It will record the ongoing security measures for physical and digital filing systems. Confirmation of compliance by third parties accessing any school user data will be recorded.
In broad terms the school will record which data has been processed (including deletions when data should no longer be stored) on which legal basis.
Consent replies are recorded within the system.

## Sharing Data

Personal data may be shared with third parties to

- Protect the vital interests of a child
- Protect the vital interests of a member of staff
- To prevent or support the detection of fraud or other legal proceedings
- When required to do so by HMRC

## CCTV

CCTV is used to support the safety and security of school users. We adhere to the ICO's code of practice* for its use. Although consent is not required for its use prominent notices inform school users that CCTV is used within the school site.
**In the picture: A data protection code of practice for surveillance cameras and personal information*

## Photographs and moving images

Consent is requested from parents and staff for the use of images. Letters requesting consent outline the choices that pupils and staff may make for the use of their images.

The school may seek consent to use photographs for the following purposes:

- To support school user welfare (identity and security)
- To celebrate achievement within the classroom
- To celebrate achievement within the school
- To celebrate achievement in the printed press
- To celebrate achievement online

## The school's specific data security measures - data protection by design

A. All IT systems - mobile devices, laptops, tablets, mobile phones and any device capable of processing data, will be password protected.

B. All IT systems will be kept securely; the server and hard disks will be in a locked cabinet and the server room locked when the school is closed and at other times of reduced security; desktop computers and portable devices will be sited/stored in secure places.

C. Staff are expected to ensure the safety of their allocated school devices: devices may not be let unattended in cars at any time and they must be kept out of sight if taken home.

D. All passwords must be 'strong;' (at least 8 characters with a mixture of upper and lower case letters, numbers and symbols), the school will require regular changing of passwords.

E. No passwords will be written down or shared; advice is available on the safe storage of passwords.

F. The school will devise granulated levels of access as appropriate to staff responsibilities for access to personal data.

G. Devices that are used to process sensitive data and/or are vulnerable to theft will be secured with encryption software BitLocker

H. All emails containing personal data will use school systems and be encrypted by Bury Councils secure school email accounts.

I. All delated data will be deleted in a secure manner: physical data will be shredded and digital data will fully deleted with trash / junk emptied regularly. Hard disks no longer required will have the data on them deleted and the deletion certified by PCEdutech

J. Only data that is necessary for the effective performance of the school will be processed.

K. Data protection will be integrated into all appropriate policies and procedures (e.g. staff induction).

L. Staff will be updated with any significant interpretations or developments of the GDPR.

M. The school will have data impact assessments in place to protect vulnerable data subjects and sensitive data.

N. Data contained within an email, or attached to an email, will be transferred to a secure folder and the email deleted.

O. Physical data will be kept securely, having regard to the sensitivity of the data and the vulnerability of the data subject e.g. medical data will be accessible to those who need to support a school user's needs, but not to others. Data that is of a sensitive nature will only be accessible by those staff who need direct access such as Headteacher, Senior staff, Designated Safeguarding officer etc.

P. All school users will handle personal data with care: it will not be left unattended (unattended computers must be locked), school users will not allow others to oversee personal data (screens must be positioned with care); papers must not be left where others can see them.

Q. All computers that might be used to process data will be set to lock (a screensaver will activate) after 10 minutes of inactivity.

R. The Headteacher and/or the DPO will approve who and how personal data is stored on mobile devices. All mobile devices will have a pass code to protect any data stored on these devices.

S. All digital data that is stored will be backed up on at least password protected devices. The backup happens on a weekly basis and is stored in an encrypted cloud back up off site in line with the school's disaster recovery plan.

T. Personally owned devices will not be used for the storage of school personal data.

## Data breaches

All staff must report to a member of the SLT or the DPO any suspected data breaches (the loss, theft, unauthorised access to data etc.) immediately. It will be for the SLT/DPO to decide whether to the suspected data breach warrants reporting to the ICO. NB a data breach would include the accidental sharing of personal data via a wrongly addressed email.

## Training

All staff will receive basic training in the requirements of the GDPR. The training will be recorded in the data audit and/or the data processing records. Governors will also receive a briefing. Data protection will form a part of pupils' e-safety education. The school will keep staff and governors up to date with guidance, changes and interpretations to data protection law.

## Data Protection Impact Assessment

For the school's most sensitive data processing activities the school will have completed a DPIA to ensure that the risk to individuals of a data breach is minimised, as should be the risk to the school's reputation. Staff involved in processing the school's most sensitive data will have to record their reading and understanding of the relevant DPIA.

## Monitoring

The DPO will lead the formal monitoring of the school's compliance with the GDPR. Every member of staff and governor shares a responsibility to monitor compliance and to report any suspected failures to comply.

## Footnotes

1. Data subjects' rights include

- The right to be informed
- The right of access
- The right to object
- The right to be forgotten (this might prove impossible in the school context)
- The right of rectification (any inaccurate data must be corrected)

2. In deciding whether to pass on a suspected data breach to the ICO the DPO will consider whether the data breach might affect a person's

- Reputation
- Confidentiality
- Financial wellbeing
- A loss of control over their data
- Make them vulnerable to discrimination
- Their rights and freedoms

## Policy Monitoring, Evaluation and Review

The Headteacher and Governing Body will review this policy annually and assess its implementation and effectiveness.

**Adopted by Spring Lane School On .....**

**Chair of Governors** .....

**Headteacher** .....