****

**Data Protection Policy**

**Version:** 1.0

**Policy Date:** 25 May 2018

Approved by: The governing Body of Ladysmith Federation on 11th July 2018

Next review date: July 2019

If you require help with the interpretation of this policy, please email the Data Protection Officer at

Infant School infant.admin@ladysmithfederation.net

**Contents**

[1 Introduction and purpose 3](#_Toc515626300)

[2 Scope 3](#_Toc515626301)

[3 Definitions 3](#_Toc515626302)

[4 Roles and responsibilities 4](#_Toc515626303)

[4.1 Governing Body 4](#_Toc515626304)

[4.2 Head Teacher 4](#_Toc515626305)

[4.3 Data Protection Officer 4](#_Toc515626306)

[4.4 Employees, temporary staff, contractors, visitors 5](#_Toc515626307)

[5 Policy content 6](#_Toc515626308)

[5.1 Data Protection Principles 6](#_Toc515626309)

[5.2 Lawfulness, fairness and transparency 6](#_Toc515626310)

[5.3 Purpose limitation 8](#_Toc515626311)

[5.4 Data minimisation 8](#_Toc515626312)

[5.5 Accuracy of data 8](#_Toc515626313)

[5.6 Storage limitation and disposal of data 9](#_Toc515626314)

[5.7 Security of personal data 9](#_Toc515626315)

[5.8 Technical security measures 9](#_Toc515626316)

[5.9 Organisational security measures 9](#_Toc515626317)

[5.10 Rights of Data subjects 10](#_Toc515626318)

[5.11 Handling requests 11](#_Toc515626319)

[5.12 Data protection by design and default 11](#_Toc515626320)

[5.13 Joint controller agreements 11](#_Toc515626321)

[5.14 Data processors 12](#_Toc515626322)

[5.15 Record of processing activities 12](#_Toc515626323)

[5.16 Management of personal data breaches 12](#_Toc515626324)

[5.17 Data Protection Impact Assessments 13](#_Toc515626325)

[5.18 Appointment of a Data Protection Officer 14](#_Toc515626326)

[6 Policy history 15](#_Toc515626327)

[Declaration 16](#_Toc515626328)

[Appendix 1 17](#_Toc515626329)

# Introduction and purpose

This policy sets out Ladysmith Federation’s commitment to handling personal data in line with the EU General Data Protection Regulation 2016 and the UK Data Protection Act 2018 (collectively referred to as the data protection legislation).

The school is the data controller for the personal data it processes and is registered with the Information Commissioner’s Office (ICO) under registration number Z6178388. Details about this registration can be found at [www.ico.org.uk](http://www.ico.org.uk)

The purpose of this policy is to explain how the school handles personal data under the data protection legislation, and to inform employees and other individuals who process personal data on the school’s behalf, of the school’s expectations in this regard.

# Scope

This policy applies to the processing of personal data held by the school. This includes personal data held about pupils, parents/carers, employees, temporary staff, governors, visitors and any other identifiable data subjects.

This policy should be read alongside the federation’s record retention schedule.

# Definitions

There are several terms used in the data protection legislation and in this policy, which must be understood by those who process personal data held by the school. These are:

Personal data

Special categories of personal data

Processing

Data subject

Data controller

Data processor

These terms are explained in Appendix 1.

# Roles and responsibilities

## Governing Body

The governing body has overall responsibility for ensuring the school implements this policy and continues to demonstrate compliance with the data protection legislation.

This policy shall be reviewed by the governing body on an annual basis.

## Head Teacher

The Head Teacher has day-to-day responsibility for ensuring this policy is adopted and adhered to by employees and other individuals processing personal data on the school’s behalf.

## Data Protection Officer

The Data Protection Officer (DPO) is responsible for carrying out the tasks set out in Article 39 of the General Data Protection Regulation (the GDPR). In summary, the DPO is responsible for:

informing and advising the school of their obligations under the data protection legislation

monitoring compliance with data protection policies

raising awareness and delivering training to employees

carrying out audits on the school’s processing activities

providing advice regarding Data Protection Impact Assessments and monitoring performance

co-operating with the Information Commissioner’s Office

acting as the contact point for data subjects exercising their rights

The DPO shall report directly to the governing body and Senior Leadership Team and shall provide regular updates on the school’s progress and compliance with the data protection legislation.

The school’s DPO is an external consultant who performs the role under a service contract. The DPO is Amber Badley, who can be contacted through the school at infant.admin@ladysmithfederation.net

The DPO is supported in their role by a school employee, this person is known as the DPO’s Data Protection Link Officer. All enquiries, complaints, requests and suspected breaches of security, should be referred to the Data Protection Link Officer in the first instance, who will then notify the DPO.

The school’s Data Protection Link Officer is Jessie Hay and can be contacted at finance@ladysmithfederation.net, 01392 271596

## Employees, temporary staff, contractors, visitors

All employees, temporary staff, contractors, visitors and other individuals processing personal data on behalf of the school, are responsible for complying with the contents of this policy.

All individuals shall remain subject to the common law duty of confidentiality when their employment or relationship with the school ends. This does not affect an individual’s rights in relation to whistleblowing.

Failure to comply with this policy may result in disciplinary action or termination of employment or service contract.

# Policy content

## Data Protection Principles

The GDPR provides a set of principles which govern how the school handles personal data. In summary, these principles state that personal data must be:

processed lawfully, fairly and in a transparent manner

collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

adequate, relevant and limited to what is necessary for the purpose it was processed

accurate and where necessary kept up to date

kept for no longer than is necessary

processed in a manner that ensures appropriate security of the data

The school and all individuals processing personal data controlled by the school, shall comply with the data protection principles in the following manner:

## Lawfulness, fairness and transparency

*Lawful processing*

Personal data will only be processed where there is a lawful basis for doing so. This will be where at least one of the following applies:

The data subject has given consent

It is necessary for the performance of a contract or entering into a contract with the data subject

It is necessary for compliance with a legal obligation

It is necessary to protect the vital interests of a person

It is necessary for the performance of a task carried out in the public interest or in the exercise of official duties

When special categories of personal data are processed (for example, health or medical data, racial or ethnic origin or biometric data (e.g. facial images and fingerprints)), this shall only be done where a lawful basis has been identified from the list above, and one from the following list:

The data subject has given explicit consent

The processing is necessary for the purposes of exercising or performing any right or obligation which is imposed on the school in relation to employment, social security and social protection law (e.g. safeguarding individuals at risk; protection against unlawful acts; prevention against fraud)

It is necessary to protect the vital interests of any person where the data subject is physically or legally incapable of giving consent

The processing is necessary for the establishment, exercise or defence of legal claims

The processing is necessary in the substantial public interest

The processing is necessary for the assessment of the working capacity of the employee

*Consent*

Most of the school’s processing of personal data will not require consent from data subjects (or their parents/carers as appropriate), as the school needs to process this data in order to carry out its official tasks and public duties as a school.

However, there are circumstances when the school is required to obtain consent to process personal data, for example:

To collect and use biometric information (such as fingerprints)

To send direct marketing or fundraising information by email or text

To take and use photographs, digital or video images and displaying, publishing or sharing these in a public arena such as:

* + on social media;
	+ in the school prospectus;
	+ on the school website;
	+ in the press/ media;
	+ in the school newsletter

When the school relies on consent as its lawful basis, it shall ensure the person providing it has positively opted-in to the proposed activity and is fully informed as to what they are consenting to and any non-obvious consequences of giving or refusing that consent. Consent shall not be assumed as being given if no response has been received e.g. a consent form has not been returned.

The school shall ensure that where consent is obtained, there is a record of this. Where possible, consent shall be obtained in writing. All forms requesting consent shall include a statement informing the person of their right to withdraw, and an email address so they may notify the school of any changes or withdrawal of consent.

*Fairness and transparency*

The school shall be fair, open and transparent in the way it handles personal data, and will publish privacy notices which explain:

What personal data the school processes and why

What our lawful basis is when we process that data

Who we might share that data with

If we intend to transfer the data abroad

How long we keep the data for

What rights data subjects have in relation to their data

Who our Data Protection Officer is and how to contact them

The school’s privacy notices shall be clear, concise and easily accessible.

Privacy notices will be provided to parents/carers of pupils when their child is enrolled at the school, which will explain how the school handles pupil information. This privacy notice will be provided on an annual basis thereafter and will be published on the school’s website.

Employees will be given a privacy notice explaining how the school handles employee information when they join the school, and annually thereafter.

The school shall provide privacy notices to other categories of data subjects, as appropriate.

## Purpose limitation

The school shall collect personal data for specified (i.e. as described in the school’s privacy notices), explicit and legitimate purposes and shall not process this data in any way would could be considered incompatible with those purposes (e.g. using the data for a different and unexpected purpose).

## Data minimisation

The school shall ensure the personal data it processes is adequate, relevant and limited to what is necessary for the purpose(s) it was collected for.

## Accuracy of data

The school shall take all reasonable efforts to ensure the personal data it holds is accurate and where necessary kept up to date. Where personal data is found to be inaccurate, this information will be corrected or erased without delay.

The school will send frequent reminders, on at least an annual basis, to parents/carers, pupils and employees, to remind them to notify the school of any changes to their contact details or other information.

The school shall carry out sample checks of pupil and employee files containing personal data, to ensure the data is accurate and up to date. This will be carried out on an annual basis.

## Storage limitation and disposal of data

The school shall keep personal data for no longer than is necessary for the purpose(s) of the processing. The school shall maintain and follow a Record Retention Schedule, which sets out the timeframes for retaining personal data. This schedule shall be published alongside the school’s privacy notices on the website.

The school shall designate responsibility for record disposal/deletion to nominated employees, who shall adhere to the school’s Record Retention Schedule and ensure the timely and secure disposal of the data.

## Security of personal data

The school shall have appropriate security in place to protect personal data against unauthorised or accidental access, disclosure, loss, destruction or damage. This will be achieved by implementing appropriate technical and organisational security measures.

## Technical security measures

The school shall implement proportionate security measures to protect its network and equipment and the data they contain. This includes, but is not limited to:

having a Firewall, anti-virus and anti-malware software in place

applying security patches promptly

restricting access to systems on a ‘need to know’ basis

enforcing strong password policies; passwords shall be a minimum of 8 characters in length; changed at appropriate intervals and not shared or used by others

encrypting laptops, USB/memory sticks and other portable devices or removable media containing personal data

regularly backing up data

regularly testing the school’s disaster recovery and business continuity plans, to ensure data can be restored in a timely manner in the event of an incident

## Organisational security measures

The school will ensure the following additional measures are also in place to protect personal data:

Employees shall sign confidentiality clauses as part of their employment contract

Data protection awareness training shall be provided to employees during induction and annually thereafter

Policies and guidance shall be in place relating to the handling of personal data whilst during and outside of school. These will be communicated to employees and other individuals as necessary, including policy revisions. A policy declaration shall be signed by employees and retained on their personnel file.

Data protection compliance shall be a regular agenda item in governing body and Senior Leadership Team meetings.

Cross cutting shredders and/or confidential waste containers will be available on the school’s premises and used to dispose of paperwork containing personal data.

Appropriate equipment and guidance will be available for employees to use and follow when carrying paperwork off school premises.

The school’s buildings, offices and where appropriate classrooms, shall be locked when not in use.

Paper documents and files containing personal data shall be locked in cabinets/cupboards when not in use, and access restricted on a need to know basis.

Procedures shall be in place for visitors coming onto the school’s premises. These will include signing in and out at reception, wearing a visitor’s badge and being escorted by a school employee (unless the visitor holds a valid Disclosure and Barring Service certificate, or it is otherwise appropriate for the person not to be escorted).

The school shall have procedures in place to identify, report, record, investigate and manage personal data breaches in the event of a security incident.

## Rights of Data subjects

Data subjects have several rights under data protection legislation. The school shall comply with all written requests from data subjects exercising their rights without delay, and within one month at the latest.

Data subjects have the right to:

request access to the personal data the school holds about them and receive a copy of this information free of charge (the school reserves the right to charge for photocopying, postage and packaging);

ask for the information the school holds about them to be rectified if it is inaccurate or incomplete;

to ask in certain circumstances for the processing of their data to be restricted;

object to the school processing their information for the ‘performance of a task carried out in the public interest’, except where the school can demonstrate compelling legitimate grounds;

object to the school using their information for direct marketing purposes;

stop the school processing their data if the school relied on consent as the lawful basis for processing, and they have subsequently withdrawn consent;

complain to the school and the Information Commissioner’s Office if they are not satisfied with how their personal data has been processed;

request compensation from the school if they have suffered damage or distress as result of a breach of security involving their personal data.

## Handling requests

Data subjects exercising their rights must put their request in writing and send it to the school at Ladysmith Infant and Nursery School, Ladysmith Road, Exeter, Devon, EX1 2PS. email infant.admin@ladysmithfederation.net.

Data subjects who request a copy of their personal data (known as making a Subject Access Request) may be asked to provide identification to satisfy the school of their identity, particularly where the data subject is no longer a pupil, employee or governor at the school. These requests shall be responded to within 1 month, upon receipt of receiving the request in writing and appropriate identification (where requested).

*Pupil information requests*

Pupils can request access to their own personal data when they are over the age of 12 and have sufficient maturity to understand their rights; know what it means to make such a request and can interpret the information they receive.

Where the child attends a maintained school, a parent can request a copy of their child’s educational record. The parent/carer does not need consent from the child to access this information. This type of request is governed by the Education (Pupil Information) (England) Regulations 2005. These requests shall be responded to within 15 school days

When responding to Subject Access Requests or pupil information requests, the school shall redact the information the data subject or parent/carer is not entitled to receive, in accordance with the exemptions set out in the Data Protection Act 2018.

The school shall consult with the Data Protection Officer upon receipt of a Subject Access Request or pupil information request, and again prior to making disclosures in response to these requests.

## Data protection by design and default

The school shall have appropriate technical and organisational measures in place which are designed to implement the data protection principles in an effective manner, and will ensure that by default, it will only process personal data where it is necessary to do so. The school’s Data Protection Policy and supplementary policies, procedures and guides, explain how the school aims to achieve this.

## Joint controller agreements

The school shall sign up to agreements with other data controllers where personal data is shared or otherwise processed on a regular basis, where it is necessary to do so.

## Data processors

The school shall carry out checks with prospective data processors (e.g. suppliers providing goods or services which involve the processing of personal data on the school’s behalf) to assess they have appropriate technical and organisational measures that are sufficient to implement the requirements of the data protection legislation and to protect the rights of data subjects.

The school’s Data Protection Officer, IT Manager and Data Protection Link Officer shall assess the appropriateness of data processors before the school purchases their services. A record will be kept of their findings.

The school shall ensure there are appropriate written contracts/Terms of Service in place with data processors, which contain the relevant clauses listed in Article 28 of the GDPR.

## Record of processing activities

The school shall maintain a record of its processing activities in line with Article 30 of the GDPR. This inventory shall contain the following information:

Name and contact details of the school and its Data Protection Officer

Description of the personal data being processed

Categories of data subjects

Purposes of the processing and any recipients of the data

Information regarding any overseas data transfers and the safeguards around this

Retention period for holding the data

General description of the security in place to protect the data

This inventory shall be made available to the Information Commissioner upon request.

## Management of personal data breaches

The school shall have procedures in place to identify, report, record, investigate and manage personal data breaches (i.e. security incidents involving personal data). These include security incidents resulting in the:

unauthorised or accidental *disclosure* or *access* to personal data

unauthorised or accidental *alteration* of personal data

accidental or unauthorised *loss of access* or *destruction*of personal data

All security incidents and suspected personal data breaches must be reported to the Data Protection Officer immediately, via the school’s Data Protection Link Officer, by emailing finance@ladysmithfederation.net or telephone 01392 271596.

All incidents will be recorded in the school’s data breach log and investigated by a member of the Senior Leadership Team (or other person as appropriate), under the support and direction of the school’s Data Protection Officer.

*Notification to the ICO and Data Subjects*

The Data Protection Officer shall determine whether the school must notify the Information Commissioner’s Office and data subjects.

Where a breach is likely to result in a risk to the data subject, for example if they could suffer damage, discrimination, disadvantage or distress as a result of the breach, the school shall notify the Information Commissioner’s Office (ICO) *within 72hrs* of becoming aware of the breach.

If the breach is likely to result in ‘high risks’ to data subjects, for example if the breach could lead to identity theft, psychological distress, humiliation, reputational damage or physical harm, the school shall inform the data subject promptly and without delay.

When informing a data subject of a personal data breach involving their personal data, the school shall provide in clear, plain language the:

nature of the incident

name and contact details of the Data Protection Officer

likely consequences of the breach

actions taken so far to mitigate possible adverse effects

## Data Protection Impact Assessments

The school shall carry out Data Protection Impact Assessments (DPIAs) on all processing of personal data, where this is likely to result in high risks to the rights and freedoms of data subjects, particularly when using new technologies. This includes, but is not limited to the following activities:

Installing and using Closed Circuit Television (CCTV)

Collecting and using biometric information, such as fingerprints

Sharing personal data or special category data with other organisations

Using mobile Apps to collect or store personal data, particularly about children

Storing special category data in the ‘Cloud’

Using systems that record large volumes of personal data, particularly where data processors are involved

The results from DPIAs shall be recorded and shared with the Data Protection Officer, who will advise on any privacy risks and mitigations that can be made to reduce the likelihood of these risks materialising. The Data Protection Officer will monitor the outcome of the DPIA, to ensure the mitigations are put in place.

## Appointment of a Data Protection Officer

The school shall appoint a Data Protection Officer to oversea the processing of personal data within the school, in compliance with Articles 37-38 of the GDPR. This person shall be designated on the basis of professional qualities and in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39 of the GDPR.

The school shall publish the contact details of the Data Protection Officer and communicate these to the Information Commissioner’s Office.

# Policy history

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy Version and Date** | **Summary of Change** | **Amended by** | **Implementation Date** |
| Version 1.0 25 May 2018 | This policy replaces the school’s existing Data Protection Policy | Amber Badley, Data Protection Officer | 11th July 2018 |

# Declaration

I confirm that I have read, understood and shall adhere to [insert school name] Data Protection Policy Version 1.0, dated 25 May 2018 and the supporting policies and procedures referred to in this policy.

|  |  |
| --- | --- |
| **Name:** |  |
| **Job title:** |  |
| **Date:** |  |
| **Signature:** |  |

*Instructions for school admin*

This declaration must be kept in an easily retrieval file. In the case of an employee, this should be kept on their personnel file.

Appendix 1

**Data Protection Policy Definitions**

|  |  |
| --- | --- |
| **Term Used** | **Summary Definition** |
| Personal data | Personal data means any information relating to an identified or identifiable living individual. This includes a name, identification number, location data, an online identifier, information relating to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual. |
| Special categories of personal data | Special categories of personal data mean personal data which reveal the racial or ethnic origin, political opinions, religious or philosophical beliefs and the trade union membership of the data subject.It also includes the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health, and data relating to an individual’s sex life or sexual orientation. |
| Processing  | Processing means any operation or set of operations which is performed on personal data, such as the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. |
| Data subject | An identifiable, living individual who is the subject of personal data. |
| Data controller | A data controller is an organisation who determines the purposes and means of the processing of personal data. |
| Data processor | A data processor is an organisation who processes personal data on behalf of a data controller, on their instruction. |