Data Protection Policy

This policy meets our legal obligations under the Data Protection Act 1998 by ensuring that we safely and securely process the information that service users and supporters share with us, especially information that is sensitive in nature.

Policy owner	RSSKL - Principal
Policy lead	Data Protection Officer (DPO) (Carol Langley)
Audience	All staff, volunteers and third party organisations or contractors that undertake work on behalf of the Rudolf Steiner School Kings Langley
Legislation and regulation	*Data Protection Act 1998*
Formally endorsed by	SMT and the Board of Trustees
Endorsement date	***11.09.17***
Next review	***31/01/18***

1 Introduction

1.1 The Rudolf Steiner School Kings Langley (RSSKL) is an independent school for girls and boys aged three to nineteen. The school follows the philosophy and curriculum developed through the works of Rudolf Steiner.

1.2 We hold and process personal information relating to pupils, parents and guardians of pupils, staff and volunteers (trustees), as well as any partner organisations. We also hold sensitive information about organisational business and finances.

1.3 This policy sets out how we will meet our obligations under the *Data Protection Act 1998* (and associated regulations) – as well as the expectations of pupils, parents and guardians of pupils, staff and volunteers (trustees) to ensure that we safely and securely process information they share with us, especially information that is sensitive in nature.

1.4 This is one of a number of policies and other guidance documents designed to support good practice in information governance and security, as well as ensuring we meet legislative and regulatory requirements. Related documents

are listed in Appendix 1. We strongly recommend that this data protection policy is read in conjunction with these documents – especially the over-arching Information Governance Policy and other information compliance documents.

2 Policy statement

Data protection standards

2.1 The RSSKL is committed to meeting its obligations under data protection legislation and will adhere to the standards set out in this document. We will:

- Observe the law and abide by the principles of data protection.
- Only use personal data in ways relevant to carrying out our legitimate purposes and functions as a school and in ways that are not prejudicial to the interests of individuals.
- Take due care in the collection and storage of all personal or sensitive data.
- Work to ensure that staff understand their responsibilities under data protection legislation and abide by it when processing data.
- Ensure that staff do not disclose data except where there are reasonable grounds, there has been consent or there is a legal requirement to do so.
- Staff will keep data accurate, timely and secure. All data processing will be done in good faith.
- Inform subjects of any processing that may not fall within our school objectives in as transparent a manner as is reasonably possible.
- Keep notifications to the Information Commissioner's Office (ICO) up to date.

Data processing

2.2 We will only process data that is relevant to the carrying out of the legitimate purposes and functions of the school in a way not prejudicial to the interest of individuals. Subjects will be informed about how we will use the data at the time of collection and, where it is practicable, will be asked to provide consent to use data.

2.3 We will ensure that data collection is as accurate as possible, given the methods used in collection. Data may be stored in many ways including but not limited to databases, ordered manual files or Word or Excel files.

2.4 Staff will be responsible for ensuring that all regular data care procedures are fully and conscientiously followed. Ordered manual files and databases will be kept up to date and archived in accordance with our retention schedules. Data no longer required for the organisation's legitimate purposes will be erased.

2.5 Data will be held in a secure environment. Data about individuals will be kept secure appropriate office security procedures or through controls over the computer network. Sensitive data will be treated with appropriate security.

2.6 Data processing will only be allowed where there is a clear rationale for the activity, as set out by the Act. Where data is passed to a third party for processing, we will

ensure appropriate controls are in place.

2.7 Sensitive data will only be processed under strict conditions, including:

> Having the explicit consent of the individual;

> Being required by law to process the data for employment purposes;

> Needing to process the information in order to protect the vital interests of the data subject or another.

Disclosures

2.8 We will not allow data collected from subjects to be disclosed to third parties except in circumstances which meet the requirements of the Act. For example, where subjects have given explicit permission for this data to be disclosed or where data is required as part of a criminal investigation. The DPO should be contacted for support and advice on disclosure of information to third parties.

Subject access

2.9 The RSSKL will provide information in response to any subject access request in line with the ICO's *Subject access code of practice*. Subject access requests entitle an individual (the subject) to be:

> Given a copy of the information an organisation holds about them;

> Told whether any personal data is being processed;

> Given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people; and

> Given details of the source of the data.

2.10 Subject access requests must be made in writing (email, fax and requests made by social media). Reasonable adjustments will be made where the subject has a disability which may make it difficult to communicate in writing.

2.11 We commit to responding to subject access requests promptly and, at most, within 40 calendar days of receipt. We reserve the right to make a charge in accordance with data protection legislation.

2.12 Staff handling subject access requests are able to do so within their own teams, but should contact the DPO if necessary for further support and particularly if the request involves disclosure of the following information:

> About a child;

> That may potentially identify a third party;

> About internal management decisions (e.g. reorganisation and redundancy);

> About negotiations with the subject;

> About legal advice and proceedings;

> About social work records or health and education records.

> The above may be considered exemptions to the subject access provisions in the Act.

Complaints and queries

2.14 We will respond to any complaints as quickly and responsively as possible and in line with our corporate Complaints, Comments and Compliments Procedure.

Incidents

2.15 Data protection and/or information security incidents should be reported in line with the Incident Reporting procedure.

New systems, processes, services, or projects

2.16 In order to maintain compliance with data protection requirements it is important that we identify early on whether any new systems, processes, services or projects are likely to impact on data protection. Specifically, we need to ask the question around personal information contained in any new systems processes, services or projects.

3 Responsibilities

3.1 The owner of this policy on behalf of the Board of Trustees is the SIRO..

3.2 The Senior Management Team (SMT) are responsible for being champions of data protection good practice in the school and ensuring compliance with policy within their teams.

3.3 The organisational lead on data protection is the DPO, who is responsible for ensuring maintenance and implementation of this policy, advising on data protection issues, liaising with the ICO and providing support on subject access requests.

3.4 It is the responsibility of all managers to ensure compliance with the policy within their area of responsibility and, in particular, to ensure that their direct reports understand the key concepts of data protection and are able to escalate subject access requests.

3.5 All staff have a responsibility to meet the obligations set out in this policy.

4 Laws and regulations

4.1 This policy meets legislative obligations under the *Data Protection Act 1998* and associated regulations.

5 Training and support

5.1 This policy supports effective risk management by setting out our expected standards in relation to data protection. In doing so, the RSSKL is taking appropriate steps to protect the information it holds and minimise the risks associated with accidental disclosure of confidential, personal or commercially sensitive information relating to pupils, parents and guardians of pupils, staff and volunteers (trustees) and partners.

6 Review and maintenance

6.1 This policy was updated in _____.

6.2 It will next be formally reviewed in January 2018, in advance of the commencement of the European Union's General Data Protection Regulations.