Roselands & Stafford Federation

# Data Protection and Information Security Policy

## Document control:

| Ratification | | | |
|---|---|---|---|
| **Signed by** | **Name** | **Signature** | **Date** |
| Headteacher | John Maxwell | | |
| Chair of Governors | Jon Nay | | |

**Distribution**

**Shared with**

- Staff via school server
- Governors via full governing body meeting
- Parents via website

**Revision history**

| Version | Revision Date | Revised By | Revision |
|---|---|---|---|
| 1 | 10.05.19 | John Maxwell | Model policy adapted as required |

**Date for next review:**

- April 2020

## 1 Introduction

1.1 Roselands and Stafford Federation collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable the school to provide education and other related services. There is also a legal requirement for schools to collect and use information to ensure that the school complies with its statutory obligations.

## 2 Definitions

2.1 Data Protection legislation places obligations on all those who process personal data and defines the following roles:-

2.1.1 *Data Controller* – the person or organisation that determines the purpose of processing i.e. decides how and why data is used. The school is therefore a data controller.

2.1.2 *Data Processors* – the person or organisation that processes data on behalf of the controller. The school is sometimes a data processor.

2.1.3 *Data Subjects* – the individuals whose information is collected and processed (for example pupils. parents, carers, members of staff)

2.1.4 *ICO* – Information Commissioner's Office

## 3 Registration

3.1 The School, as a data controller, has to register with the ICO and maintain a record of the information it holds and the purposes for which it obtains and uses personal data (including disclosure in any form to third parties). These details must be kept up to date and available for inspection by the Information Commissioner's Office.

## 4 The Information Commissioner

4.1 The Information Commissioner is the body that oversees compliance with Data Protection legislation, and has powers to force organisations to process personal data lawfully.

4.2 Where a data subject is unhappy with some aspect of the processing of their personal information they have the right to complain to the Information Commissioner.

4.3 It is recommended that any such issue should be resolved locally between the school and the individual concerned where possible. Any enquiries subsequently received from the Information Commissioner will be referred to the school's Data Protection Officer.

## 5 Purpose

5.1 This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with Data Protection and other related legislation. It applies to information held and processed by the school regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

5.2 All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities and are required to comply with this policy.

## 6 Policy statement:

6.1 Roselands and Stafford Federation is committed to ensuring that all information is collected, processed, maintained and disclosed in accordance with the principles that personal data will be:

- processed lawfully, fairly and in a transparent manner
- collected and used for specified, explicit and legitimate purposes and not further processed in an incompatible way ('*purpose limitation'*)
- adequate, relevant and limited to what is necessary for the purpose for processing ('*data minimisation'*)
- accurate and where required, rectified without delay ('*accuracy*')
- not be kept in an identifiable form for longer than necessary ('*storage limitation'*) i.e. in line with the school's retention schedule
- information must be appropriately secured/protected against unauthorised or unlawful processing, accidental loss, destruction or damage using appropriate technical or organisational measures ('*integrity and confidentiality'*). This includes:
  – *using appropriate means of transmitting data*
  – *secure storage / disposal of personal information*
  – *where processing is sub-contracted or outsourced (e.g. payroll, disposal of confidential waste paper) there must be suitable Data Protection clauses in the contract*
  See the school's Information Security Policy for more information on securing personal data.

6.2 Personal information must also:

- be processed in accordance with the rights of data subjects e.g. right of access, right of erasure, rectification, restriction, portability and the right to object to certain processing (see section 12)
- not be transferred to countries outside the European Economic Area without adequate protection

## 7 General Statement

7.1 Roselands and Stafford Federation is committed to maintaining the above principles at all times. Therefore the school will:

- Inform individuals why the information is being collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure our staff are aware of and understand our policies and procedures

## 8 Responsibilities

8.1 All employees, Governors and any other individual handling personal information on behalf of the school have a responsibility to ensure that they comply with Data Protection legislation and the school's policies.

8.2 The school ensures that all staff who are involved in processing personal data complete the school's mandatory data protection training.

## 9 The Legal Basis

9.1 The school must comply with all relevant UK and European Union legislation, including:

- Human Rights Act 1998
- Data Protection Legislation (Data Protection Act 1998, GDPR, Data Protection Act 2018)
- Freedom of Information Act 2000
- Common law duty of confidence
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Health and Safety at Work Act 1974
- Privacy and Electronic Communications (EC Directive) Regulations 2003

## 10 Information and data definitions

10.1 Information is the product of a collection of data and expressed views and opinions based upon it. It can be held and used in many forms including, but not limited to, electronic records, hard copy (paper, fiche) phone calls and conversations. For the purpose of this policy information and data can be regarded as being the same.

10.2 This policy relates primarily to any personal data i.e. data relating to individuals or personally identifiable data.

10.1.1 **Personally Identifiable data** is any data relating to an individual ('data subject) who can be identified directly or indirectly by an identifier such as name, ID number, unique pupil number, location data (e.g. address), online identifier (e.g. IP address) or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

10.1.2 **Special Category Data** is sensitive personal data (which requires extra protection) and includes any information that may identify an individual's:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- health,
- sex life/orientation
- genetic/biometric identifier

10.2 Information that is **confidential** but doesn't relate to an individual or individuals includes the following:

- School business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations
- Politically sensitive information
- Information relating to security, investigations and proceedings
- Any information which, if released, could cause problems or damage to
- individuals, the public, the school or another organisation. This could be personal,
- financial, reputation or legal damage .

## 11 Data Protection by Design

11.1 Whenever a new policy, procedure, system or database involving personal data is proposed a Data Protection Impact Assessment (DPIA) will be completed. This will be used to identify and reduce any risks to privacy and potential risks of harm to individuals through the misuse of their personal information.

11.2 The school also recognise that in some circumstances it will be mandatory to conduct a DPIA where processing is likely to result in a high risk to individuals.

## 12 Data Subject Rights

12.1 Any person wishing to exercise their rights under data protection legislation can do so by GDPR@roselands-stafford.org. Details of this can also be found on the school's website (www.roselands-stafford.org)

12.2 Requests will be processed within 1 month of receipt of the request unless the request is complex (or if multiple requests are received from the same person)

12.3 Examples of when a request may be considered complex:

- it involves retrieval and appraisal of information from multiple sources
- it involves the retrieval of large volumes of information for one data subject
    - which are difficult to separate from information relating to other data subjects
- it is one in a series of requests from the same individual
- it involves the release of third party data for which consent has been
    - refused or cannot be obtained

12.4 In these cases a 3 month deadline for responding to the request will apply. For complex requests likely to take over 1 month, the applicant will be notified of this within the initial 1 month period.

12.5 The rights are:

12.5.1 *Right of Access*

Under data protection legislation every individual has the right of access to information relating to them. This right is called Subject Access. Any person wishing to make a Subject Access request can do so by following the instructions above. Personal information will never be disclosed verbally in response to a request.

Written consent will always be required from any person nominating a third party to request information on their behalf. Parents may make requests on behalf of their children but if the child is 13 years or older, the child must also provide written consent for the parent to make the application on their behalf.

A nominated person may make an application on behalf of anyone lacking mental capacity who would otherwise have the right to request access to their records. In these circumstances, the person making the application must have proof of a valid Lasting Power of Attorney or an Enduring Power of Attorney or proof of Court-appointed Deputyship.

No information relating to any other person (other than the individual requesting the information) will be disclosed as part of a subject access disclosure.

Any information that may prejudice the prevention and detection of crime may be exempted from disclosure. There are also a number of other exemptions which may be applied and these will be explained on an individual basis.

12.5.2 *Right of erasure*

This right allows individuals to request that their personal data is deleted where there is no justification for its continued use. It only applies, however, when:

1. The data is no longer necessary for the reason(s) for which it was originally collected
2. The data subject provided consent for the school to process their data but has subsequently withdrawn this consent
3. That data subject has objected to the school processing their data and there are no overriding grounds for continuing to process it
4. The data was processed in breach of the GDPR i.e. it was unlawfully processed
5. There is a legal requirement to erase the data
6. The data was collected with parental consent when the data subject was a child and they no longer wish for their data to be held

The school will also decline a request for erasure:

1. When we have a legal obligation or it is part of our official authority to process the data
2. For public health reasons
3. For certain archiving activities
4. When we need the data in connection with a legal claim

12.5.3 *Right to rectification*

If data subjects believe that any of the personal data the school holds about them is inaccurate or incomplete they are entitled to ask for it to be rectified. This will be looked at in the context of why the school is processing the information any necessary steps will be taken to supplement the information held in order to make it complete.

12.5.4 *Right to restriction*

In certain circumstances data subjects have a right to request that we temporarily restrict processing and access to their data. This will apply:

1. Whilst establishing accuracy of data, if a data subject has contested this
2. Whilst we follow up any objection raised by a data subject to the school processing their data.
3. When data has been processed unlawfully but the data subject does not want us to erase it and have asked, instead, for us to restrict processing of the data.
4. When we no longer need the data but the data subject has advised us that they need it in connection with a legal claim.

The right to restrict data doesn't apply if:

1. The processing is necessary for the school in connection with a legal claim
2. It is necessary for the protection of another person
3. There are substantial public interest reasons for continuing to process the data

12.5.5 *Right to portability*

Data subjects have a right to request that their data be transferred electronically to another organisation.

This only applies when:

1. The data subject themselves supplied the information and provided consent for the processing; or
2. The data is being processed as part of a contract to which the data subject is party; and
3. The data is held electronically (not in paper files)

12.5.6 *Right to object*

Data subjects have the right to object to their information being processed in the following circumstances:

1. If the school has decided that processing is necessary either to
   - perform a task carried out in the public interest or
   - as part of the school's official authority or legitimate interest and the data subject feels this is not applicable.
   - Information about why the school is processing information (the legal justification) can be found in the school's privacy notice.
2. If the school retains information in defence or potential defence of a legal claim but the data subject believes there are insufficient grounds to do so.

Data subjects also have a right to object to their data being used for direct marketing purposes at any time and the school will cease processing for this purpose if an objection is raised.

If the school uses IT systems to make automatic decisions based on personal data individuals have a right to object and:

- request human intervention in the decision making
- be able to express their point of view
- obtain an explanation of how a decision has been reached
- challenge the decision

This right does not exist if the automated decision making:

- is necessary to fulfil a contract to which they are party
- is authorised by law
- the data subject has consented to the processing

Individuals also have the right to object to data being used for research purposes unless the research is being undertaken in the wider public interest which outweighs a data subject's right to privacy.

12.5.7 *Right to be Informed*

The school issues a privacy notice which explains what information the school is processing, the legal basis for this, the purpose of processing, who the information is shared with and other information required by data protection legislation. The current privacy notice is available on the school's website (www.roselands-stafford.org) or on request from Ms Oxenbury, the School Business Leader.

## 13 Breaches of Data Protection

13.1 The school has a data breach management process which all staff are aware of and have received appropriate training to help them recognise and react appropriately to data breaches. All breaches or suspected breaches of Data Protection legislation will be reported to the school's Data Protection Officer who will ensure the process is adhered to and ensure breaches are reported to the ICO where necessary.

## 14 Information security

14.1 The school's Information Security Policy covers the creation, acquisition, retention, transit, use, and disposal of all forms of information.

14.2 It applies to all employees and School Governors; it also applies to volunteers, work experience candidates, and all staff of service delivery partners and other organisations who handle information for which the school is responsible. It will form the basis of contractual responsibilities in contracts with Data Processors where reference is made to the school's Data Protection and Information Security Policy.

14.3 It is the policy of the School that:

- we will protect information from a loss of:
  - confidentiality (ensuring that information is accessible only to authorised individuals)
  - integrity (safeguarding the accuracy and completeness of information)
  - availability (ensuring that authorised users have access to relevant information when required)
  - relevance (only keeping what we need for as long as it is needed)
- we will meet all regulatory and legislative information management requirements
- we will maintain business continuity plans
- we will deliver appropriate information security training to all staff
- we will make available appropriate and secure tools to all staff
- we will report and follow-up all breaches of information security, actual or suspected

14.4 Guidance and procedures will be maintained to support this policy. These will include procedural standards for individuals with access to information.

14.5 System operating procedures will be developed and maintained to ensure compliance with this policy.

14.6 Information systems are checked regularly for technical compliance with relevant security implementation standards.

14.7 Operational systems are subjected to technical examination to ensure that hardware and software controls have been correctly implemented.

## 15 Management of Information

15.1 The School will manage information in accordance with the principles and procedures within this policy and other relevant policies and standards. The following principles apply to how we handle information in the school:

- All identifiable personal information is treated as confidential and will be handled in accordance with the relevant legal and regulatory protocols.
- All identifiable information relating to staff is confidential except where national policy on accountability and openness requires otherwise.
- Procedures will be maintained to ensure compliance with Data Protection legislation, The Human Rights Act 1998, the common law duty of confidentiality, the Freedom of Information Act 2000 and any other relevant legislation or statutory obligation.
- Information is recorded, used and stored to protect integrity so that it remains accurate and relevant at all times.

## 16 School records

16.1 We will create and maintain adequate pupil, staff and other records to meet the school's business needs and to account fully and transparently for all actions and decisions. Such records can be used to provide credible and authoritative evidence where required; protect legal and other rights of the school, its staff and those who have dealings with the school; facilitate audit; and fulfil the school's legal and statutory obligations.

16.2 Records will be managed and controlled effectively to fulfil legal, operational and information needs and obligations in the most cost-effective manner, in line with the school's Records Management and Electronic Records Management policies.

## 17 Contacts

17.1 *Data Protection Officer*
Peter Questier,
East Sussex County Council
County Hall,
St Anne's Crescent,
Lewes,
East Sussex
BN7 1U

17.2 *Office of the Information Commissioner*
The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
website: www.ico.gov.uk