DATA PROTECTION POLICY

Person responsible:	Business Manager
Date approved by governing body:	July 2025
Review cycle:	Annually
Date of policy review:	July 2026

Data Protection Policy for Staff

The policy should be read in conjunction with the following documents: ICT and Internet Acceptable Use Policy, Data Breach Policy and Procedure, Online Safety Policy, Information and Records Retention Policy, Information Security Policy and IT Password Policy.

1 Introduction

1.1 This policy is about your obligations under data protection legislation. Data protection is about regulating the way that St Rose's uses and stores information about identifiable people (Personal Data). It also gives people various rights regarding their data - such as the right to access the Personal Data that St Rose's holds on them.

1.2 We will collect, store and process Personal Data about our staff, students, parents, suppliers and other third parties. We recognise that the correct and lawful treatment of this data will maintain confidence in St Rose's and will ensure that St Rose's operates successfully.

1.3 You are obliged to comply with this policy when processing Personal Data on our behalf. Any breach of this policy may result in disciplinary action.

1.4 The Business Manager is responsible for helping you to comply with St Rose's obligations. All queries concerning data protection matters should be raised with the Business Manager.

2 Application

2.1 This policy is aimed at all staff working at St Rose's (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities, which includes employees, governors, contractors, agency staff, work experience students and volunteers.

2.2 This policy does not form part of your contract of employment and may be amended by St Rose's at any time.

During or after your employment with us, you must not disclose any trade secrets or any information of a confidential or sensitive nature about:

St Rose's school; or

any of our service users; or

any of our employees.

There is an exception if you need to share this information as part of your job or if you are made to by law.

2.3 It is the responsibility of all staff to ensure data security. You will be responsible for the confidentiality, integrity, and availability of all data which you have access to in the course of your work.

3 What information falls within the scope of this policy

3.1 Data protection concerns information about individuals.

3.2 Personal Data is data which relates to a living person who can be identified either from that data, or from the data and other information that is available.

3.3 Information as simple as someone's name and address is their Personal Data.

3.4 For you to do your job, you will need to use and create Personal Data. Virtually anything might include Personal Data.

3.5 Examples of places where Personal Data might be found are:

3.5.1 on a computer database;

3.5.2 in a file, such as a student report;

3.5.3 a register or contract of employment;

3.5.4 student health records; and

3.5.5 email correspondence.

3.6 Examples of documents where Personal Data might be found are:

3.6.1 a report about a child protection incident;

3.6.2 a record about disciplinary action taken against a member of staff;

3.6.3 photographs of students;

3.6.4 contact details and other personal information held about students, parents and staff and their families;

3.6.5 contact details of a member of the public who is enquiring about placing their child at St Rose's;

3.6.6 information on a student's performance; and

3.6.7 an opinion about a parent or colleague in an email.

3.7 These are just examples - there may be many other things that you use and create that would be considered Personal Data.

3.8 **Categories of Critical Personal Data:** The following categories are referred to as **Critical Personal Data** in this policy and in the Information Security policy. You must be particularly careful when dealing with Critical Personal Data which falls into any of the categories below:

3.8.1 information concerning child protection and child and adult safeguarding matters;

3.8.2 information about serious or confidential medical conditions and information about special educational needs;

3.8.3 information concerning serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved);

3.8.4 financial information (for example about parents and staff);

3.8.5 information about an individual's racial or ethnic origin;

3.8.6 political opinions;

3.8.7 religious beliefs or other beliefs of a similar nature;

3.8.8 trade union membership;

3.8.9 physical or mental health or condition;

3.8.10 sexual life;

3.8.11 genetic information;

3.8.12 information relating to actual or alleged criminal activity; and

3.8.13 biometric information (e.g. a student's fingerprints following a criminal investigation).

3.9 If you have any questions about your processing of these categories of Critical Personal Data please speak to the Business Manager.

4 Your obligations

4.1 Personal Data must be processed fairly, lawfully and transparently

4.1.1 What does this mean in practice?

(a) "Processing" covers virtually everything which is done in relation to Personal Data, including using, disclosing, copying and storing Personal Data.

(b) People must be told what data is collected about them, what it is used for, and who it might be shared with, unless it is obvious. They must also be given other information, such as, what rights they have in their information, how long we keep it for and about their right to complain to the Information Commissioner's Office (the data protection regulator).

This information is often provided in a document known as a privacy notice or a transparency notice. Copies of St Rose's privacy notices can be obtained from the Business Manager or accessed on St Rose's website. You must familiarise yourself with St Rose's Student, Parent and Staff Privacy notices.

(c) If you are using Personal Data in a way which you think an individual might think is unfair please speak to the Business Manager.

(d) You must only process Personal Data for the following purposes:

(i) ensuring that St Rose's provides a safe and secure environment;

(ii) providing pastoral care;

(iii) providing education, therapy and care for our students;

(iv) providing additional activities for students and parents (for example activity clubs);

(v) protecting and promoting St Rose's interests and objectives (for example fundraising);

(vi) safeguarding and promoting the welfare of our students; and

(vii) to fulfil St Rose's contractual and other legal obligations.

(e) If you want to do something with Personal Data that is not on the above list, or is not set out in the relevant privacy notice(s), you must speak to the Business Manager. This is to make sure that St Rose's has a lawful reason for using the Personal Data.

(f) We may sometimes rely on the consent of the individual to use their Personal Data. This consent must meet certain requirements and therefore you should speak to the Business Manager if you think that you may need to obtain consent.

4.2 **You must only process Personal Data for limited purposes and in an appropriate way.**

4.2.1 What does this mean in practice?

(a) For example, unsuccessful job applicants are told that their information will be held on file pending future job opportunities for six months. This information should not be used for any other purpose, e.g. fund-raising.

4.3 **Personal Data held must be adequate and relevant for the purpose**

4.3.1 What does this mean in practice?

(a) This means not making decisions based on incomplete data. For example, when writing reports, you must make sure that you are using all the relevant information about the student.

4.4 **You must not hold excessive or unnecessary Personal Data**

4.4.1 What does this mean in practice?

(a) Personal Data must not be processed in a way that is excessive or unnecessary. For example, you should only collect information about a parent's status with regards to the receipt of benefits so that St Rose's is able to claim Pupil Premium on behalf of students.

4.5 **The Personal Data that you hold must be accurate**

4.5.1 What does this mean in practice?

(a) You must ensure that Personal Data is complete and kept up to date. For example, if a parent notifies you that their contact details have changed, you should update St Rose's information management system.

4.6 **You must not keep Personal Data longer than necessary**

4.6.1 What does this this mean in practice?

(a) St Rose's has an Information and Records Retention policy about how long different types of data should be kept for and when data should be destroyed. This applies to both paper and electronic documents. You must be particularly careful when you are deleting data.

(b) Please speak to the Business Manager for guidance on the retention periods and secure deletion.

4.7 **You must keep Personal Data secure**

4.7.1 You must comply with the following policies and guidance relating to the handling of Personal Data:

(a) Information Security policy;

(b) ICT and Internet Acceptable Use Policy; and

(c) Information and Records Retention policy.

4.8 **You must not transfer Personal Data outside the EEA without adequate protection**

4.8.1 What does this mean in practice?

(a) If you need to transfer personal data outside the UK, please contact the Business Manager. For example, if you are arranging a trip to a country outside the UK.

5 Sharing Personal Data outside St Rose's - dos and don'ts

5.1 Please review the following dos and don'ts:

5.1.1 **DO** share Personal Data on a need to know basis - think about why it is necessary to share data outside of St Rose's - if in doubt - always ask your Line Manager.

5.1.2 **DO** encrypt emails which contain Personal Data. For example, encryption should be used when sending student information to Local Authority professionals. A system such as Egress can be used, or the encryption options in Outlook.

5.1.3 **DO** make sure that you have permission from the Business Manager or Principal to share Personal Data on St Rose's website.

5.1.4 **DO** be aware of "blagging". This is the use of deceit to obtain Personal Data from people or organisations. You should seek advice from the Business Manager or Principal where you are suspicious as to why the information is being requested or if you are unsure of the identity of the requester (e.g. if a request has come from a parent but using a different email address).

5.1.5 **DO** be aware of phishing. Phishing is a way of making something (such as an email or a letter) appear as if it has come from a trusted source. This is a method used by fraudsters to access valuable personal details, such as usernames and passwords. Do not reply to email, text, or pop-up messages that ask for personal or financial information or click on any links in an email from someone that you do not recognise. Immediately report all concerns about phishing to the IT Department.

5.1.6 **DO NOT** disclose Personal Data to the Police without permission from the Business Manager or Principal (unless it is an emergency).

5.1.7 **DO NOT** disclose Personal Data to contractors without permission from the Business Manager or Principal. This includes, for example, sharing Personal Data with an assessment software company.

6 Sharing Personal Data within St Rose's

6.1 This section applies when Personal Data is shared within St Rose's.

6.2 Personal Data must only be shared within St Rose's on a "need to know" basis.

6.3 Examples of sharing which are **likely** to comply with data protection legislation:

6.3.1 a teacher discussing a student's academic progress with other members of staff (for example, to ask for advice on how best to support the student);

6.3.2 disclosing details of a member of staff's allergy to bee stings to colleagues so that you/they will know how to respond (but more private health matters must be kept confidential).

6.4 Examples of sharing which are **unlikely** to comply with data protection legislation:

6.4.1 informing all staff that a member of staff is undergoing a disciplinary procedure

6.4.2 disclosing personal contact details for a member of staff (e.g. their home address and telephone number) to other members of staff (unless the member of staff has given permission, or it is an emergency).

6.5 You may share Personal Data to avoid harm, for example in child protection and safeguarding matters. You should have received training on when to share information regarding welfare and safeguarding issues. If you have not received this training, please contact the Designated Safeguarding Leads as a matter of urgency.

7 Individuals' rights in their Personal Data

7.1 People have various rights in their information.

7.2 You must be able to recognise when someone is exercising their rights so that you can refer the matter to the Business Manager. These rights can be exercised either in writing (e.g. in an email) or verbally.

(a) Please let the Business Manager know if anyone (either for themselves or on behalf of another person, such as their child):

(i) wants to know what information St Rose's holds about them or their child;

(ii) asks to withdraw any consent that they have given to use their information or information about their child;

(iii) wants St Rose's to delete any information;

(iv) asks St Rose's to correct or change information (unless this is a routine updating of information such as contact details);

(v) asks for electronic information which they provided to St Rose's to be transferred back to them or to another organisation;

(vi) wants St Rose's to stop using their information for direct marketing purposes. Direct marketing has a broad meaning for data protection purposes and might include communications such as St Rose's newsletter or fund-raising events information; or

(vii) objects to how St Rose's is using their information or wants St Rose's to stop using their information in a particular way, for example, if they are not happy that information has been shared with a third party.

8 Requests for Personal Data (Subject Access Requests)

8.1 One of the most exercised rights mentioned in section 7 above is the right to make a subject access request. Under this right people are entitled to request a copy of the Personal Data which St Rose's holds about them (or in some cases their child) and to certain supplemental information.

8.2 Subject access requests do not have to be labelled as such and do not even have to mention data protection. For example, an email which simply states "Please send me copies of all emails you hold about me" is a valid subject access request. You must always immediately let the Business Manager know when you receive any such requests.

8.3 Receiving a subject access request is a serious matter for St Rose's and involves complex legal rights. Staff must never respond to a subject access request themselves unless authorised to do so.

8.4 When a subject access request is made, St Rose's must disclose all that person's Personal Data to them which falls within the scope of his/her request - there are only very limited exceptions. There is no exemption for embarrassing information - so think carefully when writing letters and emails as they could be disclosed following a subject access request. However, this should not deter you from recording and passing on information where this is appropriate to fulfil your professional duties, particularly in relation to safeguarding matters.

9 Breach of this policy

9.1 A breach of this policy may be treated as misconduct and could result in disciplinary action including in serious cases, dismissal.

A member of staff who deliberately or recklessly discloses Personal Data held by St Rose's without proper authority is also guilty of a criminal offense.

10 Minimising risks to Personal Data when introducing, or changing a process, or starting a new project involving Personal Data

10.1 When the school/college is planning to change a process involving Personal Data, or a new project is started that involves processing Personal Data—such as implementing a new Management Information System (MIS) or installing CCTV—a structured approach must be followed to identify and minimise data protection risks.

10.1.1 Determine the need for a DPIA (Data Protection Impact Assessments)
The school/college must assess whether the change or project is likely to result in a high risk to individuals rights and freedoms. DPIAs are mandatory when:

(a) New technologies are used;

(b) There is large scale processing of special category data (e.g., health, financial);

(c) Systematically monitoring of individuals (e.g., CCTV, online activity) is involved;

10.1.2 Document the change or project. Your DPIA must:

(a) Describe the nature, scope, context and purpose of processing. Identify what Personal Data will be processed and define who will have access to it;

(b) Identify measures that can be put in place to eliminate or reduce risks to individuals. If you identify a high risk that you cannot mitigate, you must consult your DPO;

(c) Consult with stakeholders. You need to engage with internal stakeholders (e.g., teachers, IT staff, the DPO) and external stakeholders (e.g., parents, students, software providers);

10.1.3 Assess that the processing of Personal Data is necessary and proportionate to our purposes. You should evaluate:

(a) Whether the data processing is necessary to achieve the goal;

(b) If the data processing is proportionate to the purpose;

(c) Any alternatives that would have less risk that could achieve the same purpose

10.1.4 Agree on a schedule for reviewing DPIAs regularly:

(a) Conduct periodic reviews to ensure ongoing compliance;

(b) Update any DPIA when there is a change to the nature, scope, context and purpose of processing;

This Policy Statement is considered part of the Terms and Conditions of Employment for all staff at St. Rose's

…….. **Date ……**

Chair of Governors

…….. **Date ……**

Principal