ST BENEDICT'S SCHOOL
a minimis incipe

# Data Protection Policy

| | |
|---|---|
| Authorised by: | SET |
| Date: | January 2020 |
| Review Date: | January 2021 |
| Signature: | |

# Contents Page

## Introduction

1 **Introduction:** This policy is about your obligations under the data protection legislation. Data protection is about regulating the way that the School uses and stores information about identifiable people (**Personal Information**). Data protection legislation also gives people various rights regarding their data - such as the right to access a copy of the Personal Data that the School holds on them.

2 **Lawful treatment of data:** As a school, we will collect, store and process Personal Data about our staff, pupils, parents, suppliers and other third parties. We recognise that the correct and lawful treatment of this data will maintain confidence in the School and will ensure that the School operates successfully.

3 **In addition to this policy, you must also read the following which are relevant to data protection:**

3.1 The school's privacy notices for staff, pupils and parents;

3.2 IT acceptable use policy for staff;

3.3 The information security policy

3.4 Guidance for staff on the use of photographs and videos of pupils by the school

4 **Application:** This policy is aimed at all staff working in the School (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities, which includes employees, governors, contractors, agency staff, work experience / placement students and volunteers. Training as appropriate will be provided on a regular basis.

5 **Obligation:** 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.

6 **Queries:** The Bursar is responsible for helping you to comply with the School's obligations. All queries concerning data protection matters should be raised with the Bursar.

## What information falls within the scope of this policy?

7 **Data Protection:** Data protection concerns information about individuals.

8 **Personal Data:** 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. Information as simple as someone's name and address is their Personal Data.

9 **Personal Data at work:** In order for you to do your job, you will need to use and create Personal Data. Virtually anything might include Personal Data.

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

10.1 on a computer database;

10.2 in a file, such as a pupil report;

10.3 in a register or contract of employment;

10.4 pupils' exercise books, coursework and mark books;

10.5 health records; and

10.6 Email correspondence.

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

11.1 a report about a child protection incident;

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

11.3 School newsletters

11.4 photographs and videos of pupils;

11.5 a tape recording of a job interview;

11.6 contact details and other personal information held about pupils, parents and staff and their families;

11.7 contact details of a member of the public who is enquiring about placing their child at the School;

11.8 financial records of a parent;

11.9 information on a pupil's performance; and

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

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

12 **Critical School Personal Data:** The following categories are referred to as **Critical School Personal Data** in this policy. Critical School Personal Data is information which concerns:

12.1 Safeguarding or child protection matters;

12.2 serious or confidential medical conditions;

12.3 information about special educational needs;

12.4 financial information including parent bank details;

12.5 an individual's racial or ethnic origin;

12.6 political opinions;

12.7 religious beliefs or other beliefs of a similar nature;

12.8 trade union membership;

12.9 someone's physical or mental health or condition;

12.10 sex life including sexual orientation or gender identity;

12.11 actual or alleged criminal activity;

12.12 allegations made against an individual (whether or not the allegations amount to a criminal offence and whether or not the allegations have been proved)

12.13 biometrics (for example if the school uses a fingerprint scanner for allowing access to buildings); and

12.14 genetic information.

If you have any questions about your processing of these categories of Critical School Personal Data please speak to the Bursar.

## Your obligations

13 **Personal Data must be processed fairly, lawfully and transparently**

13.1 What does this mean in practice?

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

13.1.2 Privacy Impact Assessments must be completed prior to new projects which involve collection of new personal data.

13.1.3 People must be told what data is collected about them, what it is used for, and who it might be shared with. 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).

13.2 This information is provided in a document known as a Privacy notice. Copies of the School's Privacy notices can be obtained from the Bursar. You must familiarise yourself with all of the School's Privacy notices.

13.3 If you are using Personal Data in a way which you think an individual might think is unfair please speak to the Bursar.

14 **You must only process Personal Data for the following purposes:**

14.1 ensuring that the School provides a safe and secure environment;

14.2 providing pastoral care;

14.3 providing education and learning for our pupils;

14.4 providing additional activities for pupils and parents (for example activity clubs);

14.5 protecting and promoting the School's interests and objectives (for example fundraising);

14.6 safeguarding and promoting the welfare of our pupils; and

14.7 to fulfil the School's contractual and other legal obligations.

15 **Use of Personal Data:** 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 Bursar. This is to make sure that the School can lawfully use the Personal Data.

16 **Consent:** We may sometimes rely on the consent of the individual to use their Personal Data. Consent is generally obtained at point of admission. This consent must meet certain requirements and therefore you should speak to the Bursar if you think that you may need to obtain additional consent. If you are not an employee of the School (for example, if you are a volunteer) then you must be extra careful to make sure that you are only using personal data in a way that has been authorised by the school.

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

17.1 What does this mean in practice?

17.1.1 For example, if pupils are told that they will be photographed to enable staff to recognise them when writing references, you must not use those photographs for another purpose (e.g. in the School's prospectus). Please see the School's Code of Conduct and the Guidance for Staff on the use of Photographs and Videos of Pupils by the School for further information relating to the use of photographs and videos.

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

18.1 What does this mean in practice?

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

19 **You must not hold excessive or unnecessary Personal Data.**

19.1 What does this mean in practice?

19.1.1 Personal Data must not be processed in a way that is excessive or unnecessary. For example, you do not need to share it with all staff that a pupil has a health condition, only those staff that need to know.

20 **The Personal Data that you hold must be accurate.**

20.1 What does this mean in practice?

20.1.1 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 must ensure that the School's information management system has been updated and, as good practice, inform staff who you know have regular contact with the parent.

21 **You must not keep Personal Data longer than necessary.**

21.1 What does this this mean in practice?

21.1.1 The School has a 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 and must check the policy before doing so. You must only delete personal data if you are authorised to do so.

21.1.2 Please speak to the Bursar for guidance on the retention periods and secure deletion.

22 **You must keep Personal Data secure.**

22.1 This covers everything from making sure that confidential information is locked away and in a secure location, to choosing a long password that is difficult to guess. It also covers making sure that the information you have on laptops and smartphones is kept secure.

Security is the most important area of data protection compliance to get right. Further information on information security can be found in the

22.1.1 Information security policy; and

22.1.2 IT Acceptable use policy for Staff;

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

23.1 What does this mean in practice?

23.1.1 The EEA is the EU member states plus Iceland, Liechtenstein and Normway.

23.1.2 If you need to transfer personal data outside the EEA please contact the Bursar. For example, if you are arranging a school trip to a country outside the EEA or sending pupil information to parents who live overseas.

24 **Accountability**

24.1 The School is responsible for and must be able to demonstrate compliance with the data protection principles. You are responsible for understanding your particular responsibilities under this policy to help you ensure we meet our accountability requirements.

## Sharing Personal Data outside the School - dos and don'ts

25 **Dos and don'ts:** Please review the following dos and don'ts:

25.1 **DO** share Personal Data on a need to know basis - think about why it is necessary to share data outside of the School - if in doubt - always ask your manager.

25.2 **DO** encrypt emails which contain Critical School Personal Data described in paragraph 12 above. For example, encryption must be used when sending details of a safeguarding incident to social services.

25.3 **DO** make sure that you have permission from the Marketing Director to share Personal Data on the School website or using the School's social media accounts.

25.4 **DO** check with the bursar before using an app or other software that has not been authorised by the school.

25.5 **DO** share Personal Data in accordance with the School's Safeguarding Policy. If you have any questions or concerns relating to Safeguarding, you must contact The School Senior DSL (Designated Safeguarding Lead).

25.6 **DO** be aware of "blagging". This is the use of deceit to obtain Personal Data from people or organisations. You must seek advice from the Bursar 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).

25.7 **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. Don't 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 don't recognise or if you have any concerns about the message. You must report all concerns about phishing to the IT department immediately.

25.8 Further information on Blagging and Phishing can be found in the Information Security Policy

25.9 **DO NOT** disclose Personal Data to the Police without permission from the Bursar (unless it is an emergency).

25.10 **DO NOT** disclose Personal Data to third parties without permission from the Bursar. This includes, for example, sharing Personal Data with an external marketing team to carry out a pupil recruitment event.

## Sharing Personal Data within the School

26 **Sharing Personal Data:** This section applies when Personal Data is shared within the School.

27 **Need to know basis:** Personal Data must only be shared within the School on a "need to know" basis.

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

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

27.2 sharing personal Data in accordance with the School's Safeguarding Policy;

27.3 informing an exam invigilator that a particular pupil suffers from panic attacks; and

27.4 disclosing details of a teaching assistant'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).

Examples of sharing which are **unlikely** to comply with the Act:

27.5 the Headteacher being given access to all records kept by nurses working within the School (seniority does not necessarily mean a right of access);

27.6 a member of staff looking at a colleague's HR records without good reason. For example if they are being nosey or suspect their colleague earns more than they do. In fact accessing records without good reason can be a criminal offence (see paragraph 37 below)

27.7 informing all staff that a pupil has been diagnosed with dyslexia (rather than just informing those staff who teach the pupil); and

27.8 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).

28 **Sharing of Personal Data and safeguarding**: 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 Mr L Ramsden as a matter of urgency.

## Individuals' rights in their Personal Data

29 **Rights:** People have various rights in their information. You must be able to recognise when someone is exercising their rights so that you can refer the matter to the Bursar. These rights can be exercised either in writing (e.g. in an email) or orally.

30 **Individual's rights:** Please let the Bursar know if anyone (either for themselves or on behalf of another person, such as their child):

30.1 wants to know what information the School holds about them or their child;

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

30.3 wants the School to delete any information;

30.4 asks the School to correct or change information (unless this is a routine updating of information such as contact details);

30.5 asks for personal data to be transferred to them or to another organisation

30.6 wants the School 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 the School newsletter or alumni events information; or

30.7 objects to how the School is using their information or wants the School 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.

31 Please note, a person may be committing a criminal offence if they alter, block, erase, destroy or conceal information to prevent it from being disclosed (for example, to prevent its disclosure if a subject access request for that information has been received). Therefore if you are asked to provide information or documents to a colleague at the school who is preparing a response to a request for information then you must make sure that you provide everything.

## Requests for Personal Data (Subject Access Requests)

32 **The right to request Personal Data:** One of the most commonly exercised rights mentioned in section 0 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 the School holds about them (or in some cases their child) and to certain supplemental information.

33 **Form of request:** 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 Bursar know when you receive any such requests.

34 **If you receive a Subject Access Request:** Receiving a Subject Access Request is a serious matter for the School and involves complex legal rights. Staff must never respond to a subject access request themselves unless authorised to do so.

35 **Disclosure:** When a Subject Access Request is made, the School must disclose all of 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 unprofessional comments or embarrassing information - so think carefully when writing comments about people as they could be disclosed following a Subject Access Request. However, this must not deter you from recording and passing on information where this is appropriate to fulfil your professional duties, particularly in relation to safeguarding matters.

## Breach

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

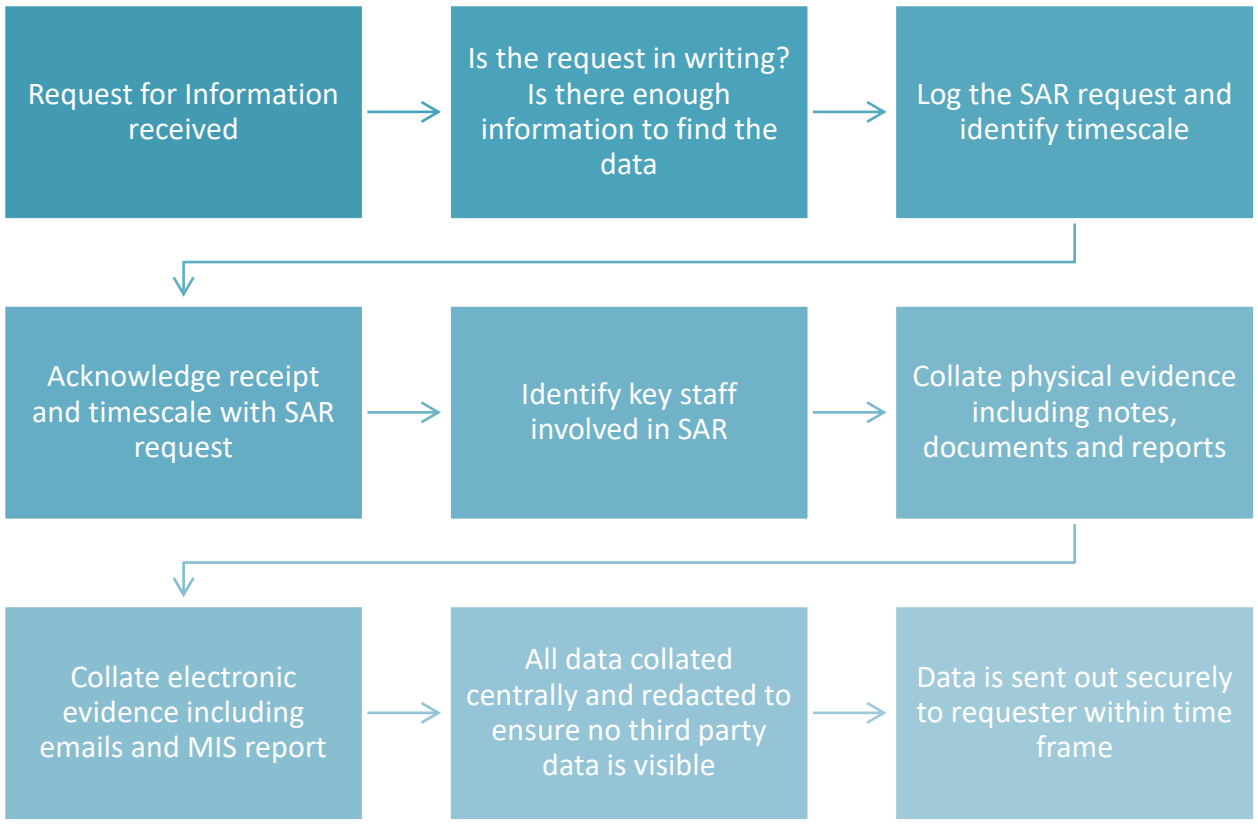
37 **Criminal Offence:** A member of staff who deliberately or recklessly discloses Personal Data held by the School without proper authority is also guilty of a criminal offence. In some cases, it can also be an offence to re-identify information which has been de-identified. Please speak to the Bursar before doing this.

## Appendix – Privacy Impact Assessment

| PRIVACY IMPACT ASSESSMENT FOR | |
|---|---|
| **You need a PIA if:-** | |
| **1** | The data collection involves the collection of new information about individuals |
| **2** | The data collection compels individuals to provide information about themselves |
| **3** | If information about individuals is to be disclosed to organisations or people who have not previously had routine access to the information? |
| **4** | You intend using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? |
| **5** | The data collection involves you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition. |
| **6** | Will the data collection result in you making decisions or taking action against individuals in ways that can have a significant impact on them? |
| **7** | Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private. |
| **8** | Will the data collection require you to contact individuals in ways that they may find intrusive? |

If you need a PIA, please contact the Bursar's Office.

## Appendix – SAR Process



**Appendix – Data Breach Process**