Data Protection Policy and Compliance Procedures for Staff

St John's School
LEATHERHEAD

Date of Issue:	28 March 2018, updated June 2019
Date of Review:	August 2020
Responsible Person:	Operations and Compliance Director
References:	Information Security Policy (L5) Information and Record Retention Policy and Procedures (L43) Privacy Notices for Staff, Pupils, Parents and Alumni Monitoring Policy (L44)
Policy Number:	L19

Data Protection Policy – General Statement of Compliance

St John's School is committed to treating individuals' personal data in a lawful manner in compliance with applicable data protection laws.[1] The School is registered with the Information Commissioner's Office. St John's School observes the principles of data protection laws when collecting, storing, using and disposing of personal data relating to members of staff (permanent, temporary or visiting), volunteers, applicants, parents, pupils (and their siblings) and alumni.

This policy statement, which is periodically reviewed and updated as appropriate, is issued to all staff and supplemented by additional policies, practices and procedures as appropriate from time to time which are intended to put this policy into effect.

The Head and Governing Council consider adherence to this policy and the fair and lawful processing of personal data to be of the utmost importance. All members of staff are expected to apply this policy, and the practices and procedures applicable to it, in their day to day activities and to seek guidance from the Operations and Compliance Director where appropriate.

1 Introduction

1.1 These procedures set out the framework for compliance with UK data protection laws as set out in the Data Protection Policy above. Data protection is about regulating the way that the School 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 the School holds on them.

1.2 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

[1] Data Protection Act 1998 as superseded by General Data Protection Regulation 2016/679 (May 2018)

will maintain confidence in the School and will ensure that the School operates successfully, and in accordance with its Data Protection Policy.

1.3 Staff are obliged to comply with these procedures when processing Personal Data on the School's behalf.

1.4 The Operations and Compliance Director is responsible for helping you to comply with the School's obligations. All queries concerning data protection matters should be raised with the Operations and Compliance Director.

2 Application

2.1 This document 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, pupils and volunteers.

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 All staff will need to use and create Personal Data in order to carry out their day to day job. . Virtually any information might include Personal Data.

3.5 Staff should be aware of those places where Personal Data might be found :

3.5.1 on a computer database;

3.5.2 in a file, such as a pupil report;

3.5.3 a register or contract of employment;

3.5.4 pupils' exercise books, coursework and mark books;

3.5.5 health records; and

3.5.6 email correspondence.

3.6 Staff should be aware of documents where Personal Data might be found. Examples include:

3.6.1 a report about a safeguarding or child protection incident;

3.6.2 staff appraisal or performance review

3.6.3 pupil lists with exam results

3.6.4 Personal development plans (PLPs)

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

3.6.6 photographs of pupils;

3.6.7 a tape recording of a job interview;

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

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

3.6.10 financial records of a parent;

3.6.11 information on a pupil's performance; and

3.6.12 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 Staff should have particular regard to the need for security when dealing with Personal Data which falls into any of the categories below (known as Critical School Personal Data):

3.8.1 information concerning child protection 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 pupil's fingerprints following a criminal investigation).

3.9 Staff must have regard to the separate Information Security Policy. If you have any questions about your processing of these categories of Personal Data please speak to Carol Robinson, Operations and Compliance Director.

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) Individuals 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 the right to complain to the Information Commissioner's Office (the data protection regulator).

This information is provided in a document known as a privacy notice to staff, parents and pupils. Copies of the School's privacy notices can be obtained from Carol Robinson, Operations and Compliance Director and accessed on the School's website. Staff should familiarise themselves with the content of these notices.

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

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

(i) ensuring that the School provides a safe and secure environment;

(ii) providing pastoral care;

(iii) providing education and learning for our pupils;

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

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

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

(vii) to fulfil the School's contractual and other legal obligations.

(e) Staff seeking to do something with Personal Data that is not on the above list, you must speak to Carol Robinson. This is to make sure that the School has a lawful reason for using the Personal Data.

(f) The School 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 Carol Robinson 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, if pupils are told that they will be photographed to enable staff to recognise them when writing references, you should not use those photographs for another purpose (e.g. in the School's prospectus).

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 of the relevant information about the pupil.

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 pupil's siblings if that Personal Data has some relevance, such as allowing the School to determine if a sibling fee discount is applicable.

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 iSAMS or contact a member of staff who can do this for you.

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

4.6.1 What does this this mean in practice?

(a) 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.

(b) Please speak to Carol Robinson, Operations and Compliance Director 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 School policies and guidance relating to the handling of Personal Data:

(a) Information Security Policy

(b) Policy on the use of photographs and videos of pupils (within E-Safety and Safeguarding and Protecting Children Policy and Procedures)

(c) IT Acceptable Use Policy for staff; and

(d) Information and Records Retention Policy and Procedure.

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

4.8.1 What does this mean in practice?

(a) This would be relevant where, for example, the School needs to send pupil information to parents living overseas, or where you access your emails whilst on holiday outside of the EEA, or use Cloud based storage. Where it is necessary to do any of the above please contact Jon Sawers, IT Network Manager.

5 Sharing Personal Data outside the School - 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 the School - if in doubt - always ask your line manager.

5.1.2 **DO** encrypt emails which contain Critical School Personal Data described in paragraph 3.8 above. For example, encryption should be used when sending details of a safeguarding incident to social services.

5.1.3 **DO** make sure that you have permission from your Carol Robinson, Operations and Compliance Director to share Personal Data on the School 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 Carol Robinson, Operations and Compliance Director 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. 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. Report all concerns about phishing to the IT department.

5.1.6 **DO NOT** disclose Personal Data to the Police without permission from Carol Robinson, Operations and Compliance Director (unless it is an emergency).

5.1.7 **DO NOT** disclose Personal Data to contractors without permission from Carol Robinson, Operations and Compliance Director. This includes, for example, sharing Personal Data with an external marketing team to carry out a pupil recruitment event. A special contract may need to be put in place to protect the security of the data concerned.

6 Sharing Personal Data within the School

6.1 This section applies when Personal Data is shared within the School.

6.2 Personal Data must only be shared within the School on a "need to know" basis.

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

6.3.1 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);

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

6.3.3 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).

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

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

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. The circumstances in which this may occur are set out in the Safeguarding and Protecting Children Policy and Procedures.

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 Carol Robinson, Operations and Compliance Director.

(a) Please let Carol Robinson, Operations and Compliance Director know if anyone (either for themselves or on behalf of another person, such as their child):

(i) wants to know what information the School 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 the School to delete any information;

(iv) asks the School 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 the School to be transferred back to them or to another organisation;

(vi) 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

(vii) 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.

8 Requests for Personal Data (Subject Access Requests)

8.1 One of the most commonly 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 the School holds about them or in some cases their child.

8.2 Specifically, people are entitled to know:

8.2.1 whether the School is holding Personal Data which relates to them or in some cases their child;

8.2.2 what that information is i.e. to receive a copy of their Personal Data;

8.2.3 the source of the Personal Data;

8.2.4 how the School uses the Personal Data; and

8.2.5 who the Personal Data has been disclosed to.

8.3 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 Carol Robinson, Operations and Compliance Director know when you receive any such requests.

8.4 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.

8.5 When a subject access request is made, the School must disclose all of that person's Personal Data to them - there are only very limited exceptions. There is no exemption for embarrassing information - so think carefully when writing letters and emails as their contents could be disclosed following a subject access request.

8.6 Parents may sometimes ask for data about their child and in some circumstances the School must ask for the child's consent to release this data. Reference should always be made to the Operations and Compliance Director for advice.

9 Breach of this policy

9.1 Any breach of this policy will be taken seriously and may result in disciplinary action.

9.2 A member of staff who deliberately or recklessly discloses Personal Data held by the School without proper authority is guilty of a criminal offence and gross misconduct. This could result in summary dismissal.