



## **Data Protection Policy for Staff**

DJJK

Apr 2018

## Review and Amendment Record

Date	Person Conducting the Review	Changes Made
Mar 2018	PMS	New Policy, GDPR
Apr 2018	DJJK	Review

## 1 Introduction

- 1.1 This policy applies to 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. This policy is about your obligations under the data protection legislation.
- 1.2 Data protection is about regulating the way 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 the School holds on them.
- 1.3 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.
- 1.4 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.
- 1.5 The School has a number of documents relating to the handling of personal data and these are indicated at Appendix A.
- 1.6 The Operations Director is the Data Protection Lead and is responsible for helping you to comply with the School's obligations. All queries concerning data protection matters should be raised with the Operations Director. Working in support of the Data Protection Lead and responsible for Privacy Impact Assessments (PIAs) in their areas of responsibility are:

Information	Responsible
Admissions, marketing	External Relations Director
Fundraising	External Relations Director
Staff and HR Management	HR manager
Academic reporting and records	Director of Studies
Medical records and reporting	Senior Sister
Financial and fees	Finance Manager
Physical data protection	ICT network Manager

## 2 Application

- 2.1 This policy does not form part of your contract of employment and may be amended by the School at any time.

## 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 In order 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 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 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 pupils;
  - 3.6.4 contact details and other personal information held about pupils, 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 the School;
  - 3.6.6 financial records of a parent;
  - 3.6.7 information on a pupil's performance; and
  - 3.6.8 an opinion about a parent or colleague in an email.
- 3.7 This list is not exhaustive - there may be many other processes that you use and create that would use Personal Data.
- 3.8 You must be particularly careful when dealing with Personal Data which falls into any of the categories below:
  - 3.8.1 information concerning child protection matters;
  - 3.8.2 information about serious or confidential medical conditions and information about additional 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. an overseas pupil's biometric identity card).

3.9 These categories are referred to as School Special Category Data in this policy and in the Information Security Policy. If you have any questions about the processing of these categories of Personal Data, please speak to the Operations 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) 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 the School's privacy notices can be obtained from the Operations Director or accessed on the School's website. You must familiarise yourself with the School's 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 Operations Director.

(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) 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 notices, you must speak to the Operations Director. This is to make sure the School 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 Operations Director if you think 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 there is CCTV in an ICT classroom for monitoring pupils' behaviour it should not be used to monitor the efficiency of cleaning staff.

#### 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 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.

#### 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 the School's information management system.

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

##### 4.6.1 What does 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 the Operations 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;
- (c) IT acceptable use policy for staff; and
- (d) 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) The School has safeguards in place for transfers outside of the EEA which relate to our routine activities. 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.
- (b) However, if you need to transfer personal data outside the EEA for less routine reasons please contact the Operations Director. For example, if you are arranging a school trip to a country outside the EEA.

## 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 Head of Department or the Operations Director.
- 5.1.2 **DO** seek advice about encrypting emails for the purpose of data transfers.
- 5.1.3 **DO** make sure that you have permission from your Head of Department or manager and the External Relations 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 the Operations 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 ICT Network Manager.
- 5.1.6 **DO NOT** disclose Personal Data to the Police without permission from the Operations Director.
- 5.1.7 **DO NOT** disclose Personal Data to contractors without permission from the Operations Director. This includes, for example, sharing Personal Data with an external marketing team to carry out a pupil recruitment event.

## 6 **Sharing Personal Data within the School**

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

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

- 6.2.1 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);
- 6.2.2 informing an exam invigilator that a particular pupil suffers from panic attacks; and
- 6.2.3 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).

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

- 6.3.1 the Operations Director being given access to payroll records on the basis of seniority alone - seniority does not necessarily mean a right of access;
- 6.3.2 using the school database to extract parent addresses for private commercial purposes unrelated to the school.
- 6.3.3 informing all staff that a pupil has been diagnosed with dyslexia (rather than just informing those staff who need to know and teach the pupil); and
- 6.3.4 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).

- 6.4 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 your school Designated Safeguarding Lead.

## **7 Individuals' rights concerning their Personal Data**

- 7.1 People have various rights concerning 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 Operations Director.

- (a) Please let the Operations Director know immediately 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 e.g. bank details, health record (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 OS 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 (SAR). 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 supplementary information.

- 8.2 SARs 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 SAR. You must always let the know Operations Director immediately when you receive any such requests because the School is required to act within a strict timeframe as set out by law.

- 8.3 Receiving a SAR is a serious matter for the School and involves complex legal rights. Staff must never respond to a SAR themselves unless authorised to do so.

- 8.4 Please be mindful 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 Please report any breach of this policy; this will be taken seriously.

9.2 A member of staff who deliberately or recklessly discloses Personal Data held by the School without proper authority maybe guilty of a criminal offence and gross misconduct.

Appendix

A. Summer Fields School Data Protection Documentation.

**Circulation for comment and input:**

Headmaster, Deputy Headmaster, Operations Director, Finance Director, External Relations Director, HR Manager, Finance Manager, Domestic Bursar, Senior Sister, Director of Studies, Director of Sport, Headmaster's PA, School Secretary, Head of Boarding, Designated Safeguarding Lead, Head of Pastoral Care. Operations Director.

**Publication:**

School website and school policy folder

Appendix A - Summer Fields School Data Protection Documentation

