St. Joseph's Catholic College

Data Protection Policy 2017

Monitoring

By	Review Period	Method
Full Governing body	Bi-Annual	Meeting

Ownership: Human Resources Manager
Revision History

Review	Changes	Next Review Date
January 2017	Revised Policy	January 2019

1 Introduction

1.1 This policy is about your obligations under the Data Protection Act 1998 (the **Act**). The Act regulates the way that the College uses and stores information about identifiable people. It also gives people various rights regarding their data - such as the right to access the personal data that the College holds on them.

1.2 As a school, we will collect, store and process personal data about our staff, students, parents, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the College and will ensure that the College operates successfully. 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.

1.3 The Senior HR, Training and Subsidiary Services Manager is also the Data Protection Officer (**DPO**) and is responsible for helping you to comply with the College's obligations. All queries concerning data protection matters should be raised with the DPO.

2 Application

2.1 This policy is aimed at all staff working in the College (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities which includes employees, Governors, Directors, contractors, agency staff, work experience / placement ,students and volunteers.

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

3 What information falls within the Act

3.1 The Act applies to personal information about individuals (**Personal Data**).

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 In order for you to do your job, you will need to use and create Personal Data. Virtually anything might include personal data.

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

3.4.1 on a computer database;

3.4.2 in a file, such as a student report;

3.4.3 a register or contract of employment;

3.4.4 health records;

3.4.5 students' work, exercise books and mark books; and

3.4.6 email correspondence.

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

3.5.1 a report about a child protection incident;

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

3.5.3 photographs of students;

3.5.4 a tape recording of a job interview;

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

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

3.5.7 financial records;

3.5.8 information on a student's performance; and

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

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

4 Your obligations

4.1 Personal Data must be processed fairly and lawfully.

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) you must only process Personal Data for the following purposes:

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

(ii) providing pastoral care;

(iii) providing education and learning for our students;

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

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

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

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

(c) if you want to do something with Personal Data that is not on the above list, you must speak to the DPO.

(d) you must be particularly careful when dealing with Sensitive Personal Data. Sensitive Personal Data is information about an individual's:

(i) racial or ethnic origin;

(ii) political opinions;

(iii) religious beliefs or other beliefs of a similar nature;

(iv) trade union membership;

(v) physical or mental health or condition;

(vi) sexual life; and

(vii) information relating to actual or alleged criminal activity.

You should speak to the DPO if you need to use any of this data for any purpose.

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 students 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 College'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, disciplining a student without getting the student's side of the story.

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 student hobbies if that Personal Data has some relevance (e.g. if relevant to PE lessons).

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 College'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) the College has a policy about how long you should keep data for and when data should be destroyed. Please familiarise yourself with this policy so you can apply it to the data that you use.

(b) you must be particularly careful when you are deleting data and must do so in line with the data retention policy.

4.7 You must process data in line with the data subject's rights.

4.7.1 **What does this mean in practice?**

(a) people must be told what data is collected about them, and what it is used for, unless it is obvious. This information is often provided in a document known as a privacy notice.

(b) copies of the College's privacy notices can be obtained from the DPO [• or accessed on the College's website].

4.8 You must keep Personal Data secure.

4.8.1 You must comply with the following College policies relating to the handling of Personal Data:

(a) information security policy;

(b) IT acceptable use policy; and

(c) information and records retention policy.

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

4.9.1 This would be relevant where, for example, the College needs to send student 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 [• name of contact].

5 Sharing Personal Data outside the College - 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 College - if in doubt - always ask the DPO.

5.1.2 **DO** encrypt emails which contain Sensitive Personal Data. 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 to share Personal Data on the College 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 DPO 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 the DPO (unless it is an emergency).

5.1.7 **DO NOT** disclose Personal Data to contractors without permission from the DPO. This includes, for example, sharing Personal Data with an external marketing team to carry out a student recruitment event.

6 Sharing Personal Data within the College

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

6.2 Personal Data must only be shared within the College 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 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 informing an exam invigilator that a particular student 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 Principal being given access to all records kept by nurses working within the College (seniority does not necessarily mean a right of access);

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

6.4.3 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 HR department.

7 Requests for information (Subject Access Requests)

7.1 People are entitled to know:

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

7.1.2 what that information is;

7.1.3 the source of the information;

7.1.4 how the College uses the information; and

7.1.5 who the information has been disclosed to.

7.2 People are also entitled to request a copy of the Personal Data which the College holds about them or in some cases their child. This is known as a Subject Access Request. 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 DPO know when you receive any such requests.

7.3 Receiving a Subject Access Request is a serious matter for the College and involves complex legal rights. Staff must never respond to a Subject Access Request themselves unless authorised to do so.

7.4 When a Subject Access Request is made, the College 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 they could be disclosed following a Subject Access Request.

7.5 People have a number of other rights under the Act, such as to prevent the use of their Personal Data for marketing; to ask to have inaccurate Personal Data amended; and to prevent the use of Personal Data in a way that causes them harm. If you receive a request which relates to the use of Personal Data you must promptly forward it to the DPO.

8 Breach of this policy

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

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