The Sisters of the Sacred Hearts of Jesus and Mary Personnel Handbook

Section	1	People management
Title	1.6	Data Protection
Document	1.6.1	Personnel Records & Data Protection Policy

We, Sisters of the Sacred Hearts of Jesus and Mary urged by the compassion of Christ and responsive to the anguish of people and planet, are called to help shape communities of gentleness, justice and peace that witness to the healing, liberating and empowering love of God.

Introduction

1. Our school aims to ensure that all personal data regarding staff is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018).
2. The Information Commissioner is responsible for administering the provisions of the General Data Protection Regulation 2018 (which supersedes the Data Protection Act 1998), and the Freedom of Information Act 2000.
3. Detailed guidance on how organisations make sure they are operating within the law can be found on the Information Commissioners Office (ICO) website following the link https://ico.org.uk/for_organisations . This policy and procedure cannot possibly answer all of the questions which may arise over data and data protection and as such the above website is a good resource for any issues which are not covered in this document.

Policy

4. The policy of the school is to fulfil all of its responsibilities under the 2018 General Data Protection Regulation and the 1998 Data Protection Act and comply with all six data protection principles listed in the act (as reproduced in Appendix 1).
5. The school also has a Privacy Policy for school staff and a Privacy Policy for applicants for our jobs. Please see the appropriate separate document for more details of who we share staff data with, why and how we ensure staff privacy.

Eligibility

6. All workers, employees, volunteers, job applicants and ex-employees of the school are included in this policy.

Entitlement

7. Any eligible person is entitled to have access to all of the records which the school may hold containing information on them, be they in the form of electronic data or paper records. They can also ask for certain data to be removed or corrected.
8. The school can expect that their employees will provide accurate personal data and that the employee will take responsibility for keeping this information up to date. To this end

the school will ask its employees to periodically check their records to ensure they are accurate.

Procedure – Records, Processing Data and the Data Controller

9. The processing of personal data is necessary to administer the contract of employment for each employee, as such this meets one of the conditions imposed on a data controller enabling them to process data. All employees must be made aware of the reasons for the processing of their personal data, who is doing the processing and their rights of access to data held on them. The employee must also be made aware of the conditions on which they can require the data controller to stop processing their data (a data subject notice). This is best done at induction. An 'Employee's statement of consent and rights of access' form should be completed by each employee and retained in their file. For new staff this is best done with their acceptance of an offer of employment. See Appendix 2 for a template form.
10. The school will keep only one personnel file on each person, to avoid duplication and inaccuracies between records creeping in, and also to demonstrate that there are no 'secret files' being kept on anyone.
11. The files should be organised in such a way as to keep more sensitive information separate from that which will be more widely shared, for example using file dividers. All data stored in the personnel file will be considered as 'sensitive', to avoid doubt as to what can be seen by others. An example of how to organise a personnel file can be found at **Error! Reference source not found.**.
12. Particularly sensitive documents such as records of disciplinary, capability or grievance investigations will be kept in or with, the personal file in a sealed envelope or folder marked confidential and will only be accessed by senior staff or HR staff who have been authorised to see them. Records linked to maternity, adoption, fertility treatment, gender reassignment or special leave will be sensitively dealt with and retained on a confidential section of the file.
13. Paper personal records (concerning a living person who can be identified from the record), organised in a filing system such that information can be readily accessed and identified will be classed as processed data.
14. The personnel records files will be kept in a locked cupboard, with access restricted to the management team and the school office manager/Bursar, who will authorise usage to staff who need the information contained therein.
15. The manager responsible will periodically ensure that all of the personnel records held are checked to make sure they are relevant, up to date and that things are not being kept for longer than is necessary.
16. It is more than likely that the school will hold personal information on a computer and as such will be classed as processing the data. Processing of personal data includes obtaining, keeping, using, accessing, disclosing and destroying data.
17. Given that the school is processing data, the school (or its controlling body) must appoint a 'Data Controller' who must be registered with the Information Commissioners Office. The 'person' can be the school, a department, the controlling body or even an individual.
18. The data controller must ensure that any processing of personal data for which they are responsible complies with the Act. To do this the data controller should ensure that systems are in place to make sure that the six data protection principles (Appendix 1) are followed. Failure to do so risks enforcement action, even prosecution, and compensation claims from individuals.

19. Any instances of breaches to the rules set out here protecting personal data will be dealt with using the disciplinary procedure.

Responsibilities - Data Protection Officer

20. The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.
21. The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.
22. Our DPO is [name] and is contactable via [contact details].

Responsibilities - All staff

23. Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their own personal data, such as a change of address, emergency contact details and their own telephone numbers.
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

Data protection principles

24. The GDPR is based on six data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

25. This policy sets out how the school aims to comply with these principles.

Collecting personal data

Lawfulness, fairness and transparency

26. We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:
    - The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
    - The data needs to be processed so that the school can **comply with a legal obligation**
    - The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
    - The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
    - The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
    - The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**
27. For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.
28. Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

Limitation, minimisation and accuracy

29. We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.
30. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.
31. Staff must only process personal data where it is necessary in order to do their jobs.
32. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's [record retention schedule/records management policy].

Access to Personal Data

33. Any individual has the right to ask to see the information held on them as personal data in their files. This is commonly called a subject access request (SAR). The request must be about the information contained in personal data files, rather than a right to see the documents that include that information. For further guidance on what to allow please refer to the ICO web site at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/
34. The person must submit a request to the DPO in writing, either by letter or email. The DPO will respond to the request as soon as possible but certainly within one month as prescribed by the act. See Appendix 4 for more information about how to deal with a subject access request and Appendix 5 for a sample SAR form.

35. If staff request access to references written about them by a third party then they must obtain permission from the author of the reference before the school/academy can release the reference to them. For the same reason references should be held separately in the personnel file and removed prior to an employee being given access to their file.
36. If the request is unfounded or excessive, the school may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. If the requests are judged to be unreasonable, then the school can refuse the request; if granted then an administration fee of £ [add admin fee] per request may be made depending on the circumstances and the reason for the request.
37. When the school refuses a request, we will tell the individual why and inform them of the right to complain to the ICO.

Other data protection rights

38. In addition to the right to make a subject access request and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to data processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO

CCTV

** Delete section if school does not use CCTV

39. CCTV is used in various locations around the school site. The school will adhere to ICO's code of practice or the use of CCTV. A code of practice to make sure the school is complying with the law can be found here: https://ico.org.uk/for-organisations/guide-to-data-protection/cctv/ We do not need to ask individuals permission to use CCTV, but we make it clear where individuals are being recorded. Cameras are clearly visible and accompanied by prominent sign explaining that CCTV is in use.

Record Keeping

40. When the school no longer has a need for the records, and there is no legal requirement to keep them the school will dispose of the records securely.

41. The length of time that personal data records must be kept varies, depending upon the record and the statute. To encompass most of the requirements and for good practice, the school will retain all records relating to a person's employment for 6 years. This should ensure that any employment records which may be used in an employment tribunal claim are within the time limit in which the employment tribunal claim could be made, and that tax and payroll records are retained for the time required by HM Revenue and Customs as a minimum.

42. Exceptions are;

    - Records relating to an accident at work should be kept for 12 years in case of an industrial injury claim.
    - Pension scheme investment records and pensions records should be kept for 12 years after the benefit ceases
    - Recruitment records for unsuccessful applicants should be kept for at least 6 months in case of any discrimination claims arising.
    - Records of any safeguarding investigation and the outcome should be securely and confidentially retained on the employee's personal file indefinitely, even after they leave the school/academy. After they leave the file should be sealed and marked to indicate its disposal at their normal retirement age.

Disposal of records

43. The schools policy on retention of records will be made clear in appropriate documents as well as policies and procedures, such as information for applicants, the disciplinary and grievance procedures. Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

44. For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Personal data breaches

45. The school will make all reasonable endeavours to ensure that there are no personal data breaches.

46. In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 6.

47. When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

    - A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
    - Safeguarding information being made available to an unauthorised person
    - The theft of a school laptop containing non-encrypted personal data about pupils

Freedom of Information Act

48. Publicly funded bodies are covered under the Freedom of Information (FOI) Act (2000). The act gives anybody the right to access official information held by a public body which includes schools and academies. Independent schools will need to determine if they are in receipt of public funds to determine if it covered by the FOI Act.

Appendix 1

Data Protection Principles

Article 5 of the GDPR requires that personal data shall be:

49.

50. **"THE PRINCIPLES**

1. "a) processed lawfully, fairly and in a transparent manner in relation to individuals;

2. b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

3. c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4. d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

5. e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

6. f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Principle explanations reproduced from the ICO and can be found at:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/

Appendix 2

Employee's Statement of Consent and Rights of Access Form

Name ..... School/Department .....

I acknowledge that the school will hold and process my personal data in order to fulfil the obligations imposed on it by law, for managing and developing its employees and for monitoring equal opportunities, its policies, procedures and working practices.

I understand that when processing my personal data the school will fully comply with the six data protection principles contained in the General Data Protection Regulations Data Protection Act 1998. These are those principles;

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

I understand that, subject to certain conditions, I have the right to access my personal data files held by the School. Should I wish to exercise this right I understand that I must submit an access request in writing to my line manager or the school office. Having made my request, I understand that:

- Files will be made available to me within one month of my request unless my request is complex or onerous.
- I may request that data is updated, inserted or removed if I consider any information is either not relevant, not correct and /or contains unsubstantiated opinions. These requests I will make in writing and give the reason for the request.
- At my request, documents will be photocopied and a reasonable charge may be made for this.
- I may not remove the records from the place where they are provided for my inspection.
- Third party references and correspondence will not be made available to me.
- Right to withdraw consent

Signed ..... **Date** .....

1. Please sign, date and return one copy of this statement to your Line Manager or the Business Manager
2. Please retain the other copy for your own safe keeping

Appendix 3 Personnel files

Suggested format for organising personnel files to avoid unauthorised persons seeing sensitive data. Each section to be held in an opaque folder or envelope.

Section folder heading and who is entitled to view content.	Type of document included
Application. Leadership team and HR	Initial response to job advertisement Completed application form Curriculum Vitae Qualifications and examination results proofs Offer and acceptance of employment letters References from previous employer(s) DBS check and 'Disclosure' report. Disability related provisions in the Job Description
Medical Leadership team and HR	Medical questionnaire Doctor's medical reports Results of pre-employment medical examination
Performance Management Leadership team, HR and line manager	Supervision records Appraisal records including targets
Grievance/Discipline Leadership team, HR and line manager	Incident reports – conduct, attendance etc Disciplinary warnings Outcome of disciplinary hearings Investigation reports
Absences Leadership team, line manager and HR plus finance office/payroll	Doctor's medical certificates Requests/responses for unpaid time off work Return to work after childbirth correspondence Certificate of Expected Confinement (Mat B1) Copy birth certificate/adoption papers Ante-natal care time off etc Accident/injury reports Declaration of absence/Return to Work Interview notes
Induction Leadership team, HR and line manager	Induction training checklist Mentor/supervisor reports
Development/Training Leadership team, HR and line manager	Training records Post-training assessments
Termination Leadership team and HR	Written reasons for dismissal Exit interviews References requested by prospective employers
Contract/Conditions Leadership team, HR and line manager plus finance office/payroll	Copy of Statement of Particulars of Employment Promotions, transfers, pay rises etc
Miscellaneous Leadership team, HR and line manager	Attachment of earnings orders Information concerning tax credits Copy award of child's Disability Living Allowance

Appendix 4 – Dealing with a Subject Access Request (SAR)

The following is reproduced from the Subject Access Code of Practice issued by the Information Commissioner's Office in 2018 and can be accessed from their web site: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

51. What information is an individual entitled to under the GDPR?

52. Under the GDPR, individuals will have the right to obtain:

    - confirmation that their data is being processed;
    - access to their personal data; and
    - other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see Article 15).

53. What is the purpose of the right of access under GDPR?

54. The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing (Recital 63).

55. Can I charge a fee for dealing with a subject access request?

56. You must provide a copy of the information **free of charge**. However, you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

57. You may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests.

58. The fee must be based on the administrative cost of providing the information.

59. How long do I have to comply?

60. Information must be provided without delay and at the latest within one month of receipt.

61. You will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, you must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

62. What if the request is manifestly unfounded or excessive?

63. Where requests are manifestly unfounded or excessive, in particular because they are repetitive, you can:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond.

64. Where you refuse to respond to a request, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

65. How should the information be provided?

66. You must verify the identity of the person making the request, using 'reasonable means'.

67. If the request is made electronically, you should provide the information in a commonly used electronic format.

68. The GDPR includes a best practice recommendation that, where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information (Recital 63). This will not be appropriate for all organisations, but there are some sectors where this may work well.

69. The right to obtain a copy of information or to access personal data through a remotely accessed secure system should not adversely affect the rights and freedoms of others.

70. What about requests for large amounts of personal data?

71. Where you process a large quantity of information about an individual, the GDPR permits you to ask the individual to specify the information the request relates to (Recital 63).

72. The GDPR does not include an exemption for requests that relate to large amounts of data, but you may be able to consider whether the request is manifestly unfounded or excessive

Appendix 5 - Employee Subject Access Request Form

Schools: insert your name and address

Dear *schools: insert the name of your data protection officer,*

Please provide me with the information held about me that I am entitled to under the General Data Protection Regulation. This is so I can be aware of the information you are processing about me and verify the lawfulness of the processing.

Here is the necessary information:

Name	
Relationship with the school	Please select: employee / governor / volunteer Other (please specify):
Correspondence address	
Contact number	
Email address	
Details of the information requested	Please provide me with: *Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example:* • *Your personnel file* •

If you need any more information from me, please let me know as soon as possible.

Please bear in mind that under the GDPR you cannot charge a free to provide this information, and in most cases, must supply me with the information within 1 month.

If you need any advice on dealing with this request, you can contact the Information Commissioner's Office on 0303 123 1113 or at www.ico.org.uk

Yours sincerely,

Employee Name

Appendix 6 – Dealing with a suspected breach of Data Protection Regulations

1. This information has come from the Information Commissioner at the ICO. The weblink to the full website blog is here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/ There is another useful webpage page here that responds to the myths around what to do if a breach occurs https://iconewsblog.org.uk/2017/09/05/gdpr-setting-the-record-straight-on-data-breach-reporting/.
2. The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.
3. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.
4. You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.
5. You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

What is a personal data breach?

6. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.
7. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

What breaches do we need to notify the ICO about?

8. When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.
9. In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals.

What role do processors have?

10. If your organisation uses a data processor, for example to process payroll, and this processor suffers a breach, then under GDPR. It must inform you without undue delay as soon as it becomes aware. If you use a processor, the requirements on breach reporting should be detailed in the contract between you and your processor, as required under GDPR.

What information must a breach notification to the supervisory authority contain?

11. When reporting a breach, the GDPR says you must provide:

a. a description of the nature of the personal data breach including, where possible:
b. the categories and approximate number of individuals concerned; and
c. the categories and approximate number of personal data records concerned;
d. the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
e. a description of the likely consequences of the personal data breach; and
f. a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

How do we notify a breach to the ICO?

12. To notify the ICO of a personal data breach, please see ICO website here: pages on reporting a breach.
13. For our school the supervising authority will be the Information Commissioners Office (ICO) [if you have schools in other countries within the EU this may be different – change this here].