

2. Applicable Data

- 2.1. For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address.
- 2.2. **Sensitive personal data** is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

3. Principles

- 3.1. In accordance with the requirements outlined in the GDPR, personal data will be:
 - Processed lawfully, fairly and in a transparent manner in relation to individuals.
 - 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.
 - Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
 - Accurate and, where necessary, kept up-to-date.
 - 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.
 - 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.
- 3.2. The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

4. Accountability

- 4.1. Cardinal Allen Catholic High School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.
- 4.2. The school will provide comprehensive, clear and transparent privacy policies.
- 4.3. Records of activities relating to higher risk processing will be maintained, such as the processing of activities that:
 - Are not occasional.
 - Could result in a risk to the rights and freedoms of individuals.
 - Involve the processing of special categories of data or criminal conviction and offence data.
- 4.4. Internal records of processing activities will be kept, including a risk register.
- 4.5. The school will implement measures that meet the principles of data protection by design and data protection by default, such as:
 - Data minimisation.
 - Pseudonymisation.
 - Transparency.
 - Allowing individuals to monitor processing.
 - Continuously creating and improving security features.
- 4.6. Data protection impact assessments will be used, where appropriate.

5. Data Protection Office (DPO)

- 5.1. A DPO will be appointed in order to:
 - Inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws.

- Monitor the school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

5.2. The DPO will report to the highest level of management at the school, which is the headteacher.

6. Lawful Processing

6.1. The legal basis for processing data will be identified and documented prior to data being processed.

6.2. Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for:
 - Compliance with a legal obligation (such as The Education Act 1996, School Standards and Framework Act 1998, Education Act 2002, Children and Families Act 2014).
 - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
 - For the performance of a contract with the data subject or to take steps to enter into a contract.
 - Protecting the vital interests of a data subject or another person.

6.3. Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
 - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
 - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
 - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
 - Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
 - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
 - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
 - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with article 89(1).

7. Consent

7.1. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

7.2. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

7.3. Where consent is given, a record will be kept documenting how and when consent was given.

7.4. Consent can be withdrawn by the individual at any time.

7.5. Where a child is under the age of 13, the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

8. The Right to be Informed

- 8.1. The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.
- 8.2. Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.
- 8.3. Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.
- 8.4. For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.
- 8.5. In relation to data that is not obtained directly from the data subject, this information will be supplied:
 - Within one month of having obtained the data.
 - If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
 - If the data are used to communicate with the individual, at the latest, when the first communication takes place.

9. The Right of Access

- 9.1. Individuals have the right to obtain confirmation that their data is being processed.
- 9.2. Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.
- 9.3. The school will verify the identity of the person making the request before any information is supplied.
- 9.4. A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.
- 9.5. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.
- 9.6. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.
- 9.7. All fees will be based on the administrative cost of providing the information.
- 9.8. All requests will be responded to without delay and at the latest, within one month of receipt.
- 9.9. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.
- 9.10. Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.
- 9.11. In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

10. The Right to Rectification

- 10.1. Individuals are entitled to have any inaccurate or incomplete personal data rectified.
- 10.2. Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.
- 10.3. Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.
- 10.4. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.
- 10.5. Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

11. The Right to Erasure

- 11.1. Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- 11.2. Individuals have the right to erasure in the following circumstances:
 - Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
 - When the individual withdraws their consent
 - When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
 - The personal data was unlawfully processed
 - The personal data is required to be erased in order to comply with a legal obligation
 - The personal data is processed in relation to the offer of information society services to a child
- 11.3. As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.
- 11.4. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.
- 11.5. Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

12. The Right to Restrict Processing

- 12.1. Individuals have the right to block or suppress the school's processing of personal data.
- 12.2. In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.
- 12.3. The school will restrict the processing of personal data in the following circumstances:
 - Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
 - Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual
 - Where processing is unlawful and the individual opposes erasure and requests restriction instead
 - Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim
- 12.4. If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.
- 12.5. The school will inform individuals when a restriction on processing has been lifted.

13. The Right to Data Portability

- 13.1. Individuals have the right to obtain and reuse their personal data for their own purposes across different services.
- 13.2. The school will respond to any requests for portability within one month.
- 13.3. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.
- 13.4. Where no action is being taken in response to a request, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

14. Privacy by Design and Privacy Impact Assessments

- 14.1. The school will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into processing activities.
- 14.2. Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy.
- 14.3. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

15. Data Breaches

- 15.1. The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- 15.2. The headteacher/DPO will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.
- 15.3. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.
- 15.4. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly.

16. Data Security

- 16.1. Confidential paper and digital data records will be kept secure as detailed in the Data Management and Retention Policy.

17. Publication of Information

- 17.1. Cardinal Allen Catholic High School publishes on its website information that will be made routinely available, including:
 - Policies and procedures
- 17.2. The information published is made available quickly and easily on request.
- 17.3. Cardinal Allen Catholic High School will not publish any personal information, including photos, on its website without the permission of the affected individual.

18. CCTV and Photography

- 18.1. The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.
- 18.2. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

19. Data Retention

- 19.1. Data will not be kept for longer than is necessary.
- 19.2. Unrequired data will be deleted as soon as practicable.

20. DBS Data

- 20.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.
- 20.2. Data provided by the DBS will never be duplicated.
- 20.3. Any third parties who access DBS information will be made aware of the data protection legislation, as well

as their responsibilities as a data handler.

21. Policy Review

- 21.1. This policy is reviewed every two years by the SBM and the headteacher.
The next scheduled review date for this policy is May 2020.

Cardinal Allen Catholic High School

Melbourne Avenue, Fleetwood. FY7 8AY

www.cardinalallen.co.uk

head@cardinalallen.co.uk

01253 872659

@CardinalAllen