General Data Protection Regulation (GDPR) Policy Incorporating Freedom of Information

Document Control Information

Reviewed	04/05/2022
Responsibility	Tom Scantlebury
Committee	Resources
Review Date	June 2023
Signed	

Version	DATE	DESCRIPTION
6	09/05/2019	Changes to Appendix 2, retention guidelines
7	10/06/2020	Minor amendments. Change responsibility to Tom Scantlebury.
8	16/06/2021	Reviewed with no changes
9	04/05/2022	Removal of repeated statements, processes and streamline statements to be specific. New links to ICO website

1. Scope
   a. Foundry College is committed to protecting all data that it holds relating to staff, pupils, parents and members of the Management Committee.

   b. This policy applies to the storing of all college data regardless of whether it is in paper, electronic, photographic or videographic format.

2. Legislation and guidance
   This policy meets the requirements of the Data Protection Act 2018 (which incorporates the General Data Protection Regulation) and is based on guidance published by the Information Commissioner's Office (ICO) and the Department for Education (DFE).

3. Data protection principles and categories of data
   a. The Data Protection Act 2018 sets out six data protection principles that the college must follow when processing personal data. Data must be:
      - Processed fairly, lawfully and in a transparent manner
      - Used for specified, explicit and legitimate purposes
      - Used in a way that is adequate, relevant and limited to only what is necessary
      - Accurate and, where necessary, kept up-to-date
      - Kept no longer than is necessary
      - Processed in a manner that ensures appropriate security of the data

   b. Categories of data
      i. The Data Protection Act 2018 refers to **Personal data** and **Special categories of personal data**
         - **Personal data** means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.
         - **Special categories of personal data** (previously known as 'sensitive personal data') includes race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health and sexual orientation.

      ii. Note that the DfE consider it best practice that data such as free school meal status, pupil premium eligibility, elements of special educational need, safeguarding, some behaviour data and Children's Services interactions are also treated with the same care as the special categories set out in law.

4. Roles and responsibilities
   a. College staff and The Management Committee have a duty to comply with this policy. (All staff and members of The Management Committee should note that the Data Protection Act 2018 makes provision for significant fines to be levied in the event of non-compliance.)

   b. The Data Controller is the competent authority which, alone or jointly with others determines the purpose and means of processing personal data.

   c. Data Protection Officer acts as the contact point for all Data Protection issues and queries from Data Subjects and the ICO, e.g. for Subject Access Requests and data breaches.

   d. Data processor will ensure that all third parties are compliant with the Data Protection Act 2018.

5. Data Protection documentation
   a. Privacy Notices
      i. The college will make available Privacy Notices via the college website.

   b. Consent

i. Where required, the college will seek and record specific consent from data subjects (e.g. image permissions, email marketing, biometrics).

6. Subject Access Requests/Parental requests to see the educational record of their child
   a. Under the Data Protection Act, pupils (or their parents for children under 13) have a right to request access to information the college holds about them. This is known as a Subject Access Request (SAR).

   b. The SAR process and timescales are provided by the Information Commissioners Office Time limits for responding to data protection rights requests | ICO

   c. In addition, Foundry College is mindful of Regulation 5 of the Education (Pupil Information) (England) Regulations 2005.

7. Freedom of Information
   a. The college will comply with the Freedom of Information Act 2000.

8. Children and consent for data processing
   i. The Data Protection Act regards children aged 13 and above, as mature enough to understand their data rights.

   ii. Therefore, children aged 13 and above:
   - Should give their permission where data collection and processing relies on consent, e.g. image permissions.
   - May make Subject Access Requests in their own right and must be asked for their agreement if a parent is making such a request.
   - Should be provided with Privacy Notices in an appropriate format.

9. Storage of Data
   a. The college will ensure that appropriate technical and organisational measures are in place to protect college data.

10. Retention and disposal
    a. The college has a document retention and disposal schedule, based on the retention guidelines from the Information and Records Management Society (IRMS) Toolkit for Schools and any other guidance, e.g. DfE, Local Authority. **Appendix 2**

11. Training
    a. All staff and members of the Management Committee will be provided with data protection training as part of their induction process.

    b. Data protection training, briefings and updates will also be provided for all staff and members of the Management Committee as required, but at least every two years.

12. This policy should be read in conjunction with all Foundry College policies

13. If you would like to contact the Foundry College Data Protection Officer (DPO):

Email: DPO@foundry.wokingham.sch.uk
Or by post:
Data Protection Officer
Foundry College
Budges Gardens
Wokingham
RG40 1PX
01183341510

APPENDIX 1

(a) Data breach information and procedures

Data protection breaches can be caused by a number of factors, e.g. Loss or theft of pupil, staff or Management Committee data and/or equipment or paperwork on which data is stored, inappropriate access controls allowing unauthorised use, poor data destruction procedures, human error such as sending an email to the wrong person, cyber-attack, hacking, ransom ware.

In the event of a breach, the procedures below should be followed:

1. Any data protection incident should be reported immediately to the college's DPO and Headteacher.

2. If required, appropriate actions should be taken to halt the breach, and/or prevent further breaches.

3. The DPO must report any significant data protection incidents to the ICO within 72 hours of the breach being detected, where feasible.

4. The Chair of the Management Committee should be informed as soon as possible. Other agencies as appropriate may need to be informed depending on the breach, e.g. police, Action Fraud, social services.

5. Where the breach involves the disclosure of the personal data of specific individuals, they should usually be notified.

6. Fully investigate the breach, and review all related policies and procedures to make any necessary changes.

7. Provide additional training to staff as appropriate.

8. Review whether any disciplinary action should be taken.

9. If the nature of the breach could result in adverse publicity the college may wish to prepare a statement for publication.

10. A full record should be kept of all data breaches, including all the steps taken, whether reportable or not.

Additional notes

In the event of a data breach, the following areas will need to be considered:

- The type of data and its sensitivity
- What protections were in place (e.g. encryption)
- What has happened to the data
- Whether the data could be put to any illegal or inappropriate use
- How many people are affected
- What type of people have been affected (pupils, staff members, suppliers etc.) and whether there are wider consequences to the breach.

(b) Subject Access Request (SAR) Process and Timescales

A SAR is a request for personal data about the applicant.
The format a SARs can be made;

- Verbally-Tom I would like to replace written application instead Verbally, because we will not have any evidence to prove they have requested for SARs.
- Letter
- Email

1. Clarify that this is a SAR and not some other request for information, i.e. a FOI request or an 'educational record' request.

2. Confirm the identity of the person making the request.

3. If it is unclear what information is being requested, ask for further details from the applicant.

4. Check that the information is available:
   - If the information is not available, inform the applicant.
   - If the information is available, note the date that the SAR was received or, in the case of further details being requested, the date that these were received. The college now has one calendar month to respond.

5. Check whether the information requested contains information about any third-party. If it does then undertake one, or more, of the following steps:
   - Seek permission to disclose the information from the third-party concerned.
   - Redact/summarise the information to protect the identity of the third-party.
   - Withhold the information to protect the rights of the third-party.

6. Ensure that the information to be supplied is clear and understandable, e.g. any complex codes or terms are explained.

7. Supply the information requested in an appropriate format, e.g. if the request is made electronically, the information should be provided in an electronic format.

8. Keep a record of the SAR and any information that was supplied.

(c) Freedom of Information (FOI) Process and Timescales

A FOI request may be made by any member of the general public, as they have a right to know about the activities of public authorities, which includes schools. The college will normally disclose the information requested in whole or part unless there is a clear and accepted reason not to do so.

All FOI requests must be in writing, either paper or electronic, and must contain the applicant's contact details. All requests should be directed to the DPO.

Additional Notes

- More information can be found on the Information Commissioners office website Home | ICO
- The college may charge for the cost of copying and postage, where appropriate.
- The college may refuse an entire request under various circumstances.

APPENDIX 2

The following retention guidelines are for data that has a possible risk of becoming a Data Protection issue.

Document	Retention Period	Disposal Method
Records relating to complaints dealt with by the Management Committee	6 years from date of resolution	Review that issue is not still contentious then secure disposal
Professional Development plans	Closure of the plan plus 6 years	Secure disposal
Admissions (if successful)	Date of admission plus 1 year	Secure disposal
Register of Admissions	Date of last entry plus 6 years	Review and may be kept permanently
Proofs of address supplied by parent as part of admissions process	Current year plus 1 year	Secure disposal
Supplementary information form including additional information such as religion, medical conditions	Current year plus 1 year	Secure disposal
Visitors books & signing in sheets	Current year plus 2 years then review	Secure disposal
All records leading up to the appointment of a Headteacher	Date of appointment plus 6 years	Secure disposal
All records leading up to the appointment unsuccessful staff applicants	Date of appointment of successful candidate + 6 months	Secure disposal
All records leading up to the successful applicant appointment that do not form part of their Staff Personnel file	6 months	Secure disposal
DBS checks	Should NOT be kept for more than 6 months	Secure disposal
Staff Personnel file	Termination date + 7 years	Secure disposal
Timesheets	Current year + 6 years	Secure disposal
Appraisal	Current year + 5 years	Secure disposal
Disciplinary proceedings Oral warning Written warning level 1 Written warning level 2 Final warning Case not found	Date of warning + 6 months Date of warning + 6 months Date of warning + 12 months Date of warning + 18 months No record Unless a child protection issue, dispose of documents at conclusion of the case. If child protection keep for either 10 years or until retirement whichever is the longer	Secure disposal
Records relating to accident / injury at work	Date of incident plus 12 years	Secure disposal
Maternity Pay records	Current Year plus 3 years	Secure disposal
FSM Registers	Current year plus 6 years	Secure disposal
School Meal Registers	Current year plus 3 years	Secure disposal
Pupils Education Record	DoB plus 25 years	Secure disposal
Child Protection info held on pupil file	Held in a sealed envelope for the same period of time as the file	These MUST be shredded
CP info held on separate files	DoB plus 25 years then REVIEW	These MUST be shredded
Attendance Registers	Date of entry plus 3 years	Secure disposal
Authorised absence correspondence	Current academic year plus 2 years	Secure disposal
SEND files , reviews, IEP's statements, advice and information provided to parents, accessibility strategy	Pupil DoB plus 25 years	Secure disposal
Examination Results	Current year plus 6 years	Secure disposal