St Richard Reynolds Catholic College

Policy: SRRCC Data Protection Policy

Date of publication: May 2018

Date of approval by Governing Body: June 2018

Review Date: As required

Contents

1. Aims

St Richard Reynolds Catholic College aims to ensure that all personal data collected, stored, processed and destroyed about any natural person, whether they be a member of staff, student / pupil, parent, visitor, contractor, consultant, a member of supply staff or other individual in the College is done so in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the forthcoming revised Data Protection Act 2018 (DPA 2018) as set out in the current Data Protection Bill. This policy will be reviewed in line with the implementation of this new legislation.

This policy applies to all personal data, collected, stored, processed and destroyed by St Richard Reynolds Catholic College, regardless of whether it is in paper or electronic format, or the type of filing system it is stored in, and whether the collection or processing of data was, or is, in any way automated.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. It is also based on the ICO guidance on GDPR, and information provided by the Article 29 Working Party.

It also meets the requirements of the Protection of Freedoms Act 2012, ICO's code of practice in relation to CCTV usage, and the DBS Code of Practice in relation to handling sensitive information. This policy also complies with the Education (Student / pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Data controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, following the Controller's instruction.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Consent	Freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Personal data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a • name, • an identification number, • location data,

- an online identifier or
- to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data

Personal data which is more sensitive and so needs more protection, including Information about an individual's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics
- Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes
- Health – physical or mental
- Sex life or sexual orientation
- history of offences, convictions or cautions *

* Note: whilst criminal offences are not classified as "sensitive data" within GDPR, within this policy template we have included them as such as acknowledgement of the care needed with this data set.

Processing

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processing can be automated or manual.

Data breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

St Richard Reynolds Catholic College processes personal data relating to parents, student / pupils, staff, governors, visitors and others, and therefore is a data controller and a data processor.

St Richard Reynolds Catholic College is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our College, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing Body

The Governing Body has overall responsibility for ensuring that our College complies with all relevant data protection obligations.

5.2 Data Protection Officer

The data protection officer (DPO) for St Richard Reynolds Catholic College is David Coy. The DPO can be contacted via the College Office office@srrcc.org.uk.

They are responsible for overseeing the implementation of this policy in the first instance, before reviewing our compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO will provide an annual report of St Richard Reynolds Catholic College compliance and risk issues directly to the governing board and will report to the board their advice and recommendations on College data protection issues.

The DPO is also the first point of contact for individuals whose data the College processes, and for the ICO. Full details of the DPO's responsibilities are being defined.

5.3 Principal

The Principal acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff (regardless of role) are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the College of any changes to their personal data, e.g. a change of address, telephone number, or bank details.
- Contacting the DPO:
    - 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

6. The GDPR Data protection principles

The GDPR is based on 6 data protection principles that St Richard Reynolds Catholic College must comply with.

These are that 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

This policy sets out how St Richard Reynolds Catholic College aims to comply with these key principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful basis' (legal reasons) to do so under data protection law:

- The individual (or their parent / carer when appropriate in the case of a student / pupil) has freely given clear **consent**
- The data needs to be processed so that the College can **fulfil a contract** with the individual, or the individual has asked the College to take specific steps before entering into a contract
- The data needs to be processed so that the College 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 College, 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 College or a third party (provided the individual's rights and freedoms are not overridden)

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.

These are where:

- The individual (or their parent/carer when appropriate in the case of a student / pupil) has given explicit consent.
- It is necessary to fulfil the obligations of controller or of data subject.
- It is necessary to protect the vital interests of the data subject.
- Processing is carried out by a foundation or not-for-profit organisation (includes religious, political or philosophical organisations and trade unions)
- The personal data has manifestly been made public by the data subject.
- There is the establishment, exercise or defence of a legal claim.
- There are reasons of public interest in the area of public health

- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment
- There are archiving purposes in the public interest.
- The Government has varied the definition of a special category.

If we decide to offer online services to student / pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, and we will get parental consent for this (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law, in the form of a privacy notice, which can found on the both College Website. Hard copies are available on request.

7.2 Limitation, minimisation and accuracy

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 in our privacy notices.

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.

Staff must only process personal data where it is necessary in order to do their jobs.

When personal data is longer required, staff must ensure it is deleted. This will be done in accordance with St Richard Reynolds Catholic College document retention policy (in the process of being updated as at June 2018), which will state how longer particular documents should be kept, and how they should be destroyed.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a student / pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies or services – we will seek consent as necessary before doing this where possible.
- Our suppliers or contractors need data to enable us to provide services to our staff and student / pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law, and have satisfactory security measures in place.
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so for:

- The prevention or detection of crime and/or fraud

- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our student / pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law, and will consult with affected individuals first.

9. Individuals Rights under GDPR

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to access personal information that St Richard Reynolds Catholic College or its Colleges holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject Access Requests should be submitted using a standard template, which can be obtained by the College Office.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of student / pupils at our College may be granted without the express permission of the student / pupil. This is not a rule and a student / pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification from the list below
    - passport
    - driving licence
    - utility bills with the current address

    - Birth / Marriage certificate
    - P45/P60
    - credit card or mortgage statement
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month (30 calendar days) of receipt of the request
- Will provide the information free of charge*
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or requested during school holidays. We will inform the individual of this as soon as possible, and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the student / pupil or another individual; or
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests; or
- Is contained in adoption or parental order records; or
- Is given to a court in proceedings concerning the child

*If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which would only take into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

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 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.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a student / pupil) within 15 College days of receipt of a written request.

Requests should be made in writing to the Data Protection Officer, and should include;

- Name of individual
- Correspondence address
- Contact number and email address

11. CCTV

St Richard Reynolds Catholic College uses CCTV in various locations around the various College sites to ensure they remain safe. We will adhere to the ICO's code of practice for the use of CCTV and provide training to staff in its use.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded, with security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use, and where further information can be sort.

Any enquiries about the CCTV system should be directed to DPO.

12. Photographs and videos

As part of our College activities, we may take photographs and record images of individuals within our College.

St Richard Reynolds Catholic College will obtain written consent upfront from parents / carers for photographs and videos to be taken of their child for communication, marketing and promotional materials.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

13. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data collection and processing activities. These include, but are not limited to the following organisational and technical measures:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection regulations.
- Completing data privacy impact assessments where the College's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies or processing tools. Advice and guidance will be sort from the DPO.

- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regular, at least annual training members of staff ad governors on data protection law, this policy and any related policies and any other data protection matters. Records of attendance will be kept to record the training sessions, and ensure that all data handlers receive appropriate training.
- Termly reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our College and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.
In particular our or organisational and technical measures include the following:

- Staff have been advised to lock away portable electronic devices, such as laptops, tablets and hard drives that contain personal data when not in use.
- Staff have been advised that papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access (unless there is a conflict with safeguarding, e.g. staff awareness of medical issues).
- Passwords that are at least 7 characters long containing letters and numbers are used to access College computers, laptops and other electronic devices. Staff and students / pupils are reminded to change their passwords at regular intervals.
- We are progressing plans to ensure that all USBs used at the College are encrypted and that and encryption software is required for all portable devices and removable media.
- Staff, student / pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for College-owned equipment.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (e.g. sending by USO-FX).

15. Disposal of records

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.

For example, we will shred paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the College's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law, and provide a certificate of destruction. This is then recorded on our systems.

16. Personal data breaches

The College will make all reasonable endeavours to ensure that there are no personal data breaches.
In the unlikely event of a suspected data breach, we will follow the procedure set out in St Richard Reynolds Catholic College Breach Management Policy (in the process of being updated as at June 2018).

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

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

17. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy as part of the general monitoring and compliance work they carry out. As previously stated this policy will be reviewed after one year, and then after that point it will be reviewed every two years. St Richard Reynolds Catholic College Governors will be included as part of the review process.