Data Protection Policy

POLICY ORIGINATOR	J Newton	MONITORING & EVALUATION BY	CEO
COMMITTEE RESPONSIBLE	FCAT Board	DATE APPROVED	March 2019
REVIEW CYCLE	Bi-Annual	REVIEW PERIOD	Spring 2021

FILE REFERENCE	Data Protection Policy (March 2019)

Contents

Part 1: Aims

Frassati Catholic Academy Trust (FCAT / The Trust) aim to ensure all personal data collected about staff, pupils, parents, governors, visitor and other individuals is stored and processed in accordance with the General Data Protections Regulation (GDPR) and the provisions set out in the Data Protection Act 2018 (DPA 2018

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Part 2: Legislation and Guidance

This policy meets the requirements of both the GDPR provisions and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on GDPR and its code of practice for subject access requests, use of surveillance cameras and personal information.
In addition, FCAT, at its discretion, chooses to follow regulation 5 of the Education (Pupil In=formation) (England) Regulations 20015, which gives parents the right of access to their child's educational record.

Part 3: Definitions

Term	Definition
Consent	Any 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 them.
Data Subject	The identified or identifiable individual whole personal data is held or processed.
Data Set	A group of identifiable data subjects, eg pupils, staff, parents etc.
Data Controller	A person or organisation that determines the purposes of and the means of processing of personal data.
Data Processor	A person or other body (other than an employee of the data controller), who processes data on behalf of the data controller.
Personal Data	Any information relating to an identified or identifiable individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as username t may also include factors specific to the individual's physical, physiological, genetic, economic, cultural or social identity.
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) where used for identification purposes • Health – physical or mental • Sex life or orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Personal Data	A breach of security leading to the accidental or unlawful destruction, loss,

Breach	alteration, unauthorised disclosure of, or access to personal data
Suppression List	A register recording the details of data subjects that **do not consent** to specific information being sent, emailed or coped to them.

Part 4: The Data Controller

FCAT processes personal data relating to pupils, parents, staff, governors, visitors and others, and therefore is a data controller and is registered as a data controller with the ICO and renews registration annually or as otherwise legally required.
The Trust comprises of nurseries, primary schools and the central team, across three local authorities.

Part 5: Roles and Responsibilities

This policy applies to all staff employed by FCAT and to external organisations or individuals working on its behalf. Staff who do not comply with this policy may face disciplinary action.
5.1 The Directors: The Board has overall responsibility for ensuring FCAT fully complies with all relevant data protection obligations.
5.2 Chief Executive Officer (CEO): The CEO acts as the representative of the Data Controller on a day-to-day basis.
5.3: Data Protection Officer (DPO): The DPO is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law and developing related policies and guidelines where applicable.
The DPO will report to the Audit and Risk Committee annually.
5.4 School Data Controllers (SDC). School Business Managers (or equivalent) are the SDC for each setting. They are to be the first point of contact for staff and are responsible for:

- Contacting the DPO regarding implementation of the policy,
- Contacting the DPO if there has been a data breach
- Ensuring the schools suppression list is maintained and reviewed.
- Maintaining an up to date record of the school's data processors
- The provision of certified, secure document disposal for their school.

5.5 All Staff: are responsible for
Collecting, storing and processing any personal data in accordance with this policy.
Informing the school of any changes to their personal data, such as change of address.
Contacting their SDC:

- With any questions relating to the operation of this policy
- If they have any concerns the 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.
- Report any data breaches.

Part 6: Data protection principles

GDPR s based on the following data protection principles and states 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 kept up to date.
- Kept for no longer than is necessary for the purposes for which it is processed.
- Processed in such a way that ensures it is appropriately secured.

Part 7: Collecting personal data

7.1 Lawfulness, fairness and transparency

FCAT will only process personal data where there is a lawful basis;

- 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.
- So that the school can **comply with a legal obligation**
- To ensure the **vital interest** of the individual e.g. to protect someone's life.
- So that the school, as a public authority, can perform a task **in the public interest**, and carry out its official function.
- For the **legitimate interests** of the school or a third party (provided that the individual's rights and freedoms are not overridden)
- When the individual (or parent of a pupil under 13) has freely given clear **consent.**

FCAT will not often need to use consent, however, where it is sought the following is to apply:

- Individuals are to have a positive opt-in, the use of pre-ticked boxes or any other method if default consent is not to be used.
- It is to be clear, concise, specific and granular ie separate consent is obtained for each request, vague or blanket consent is not sufficient.
- Requests for consent are to be separate from other terms and conditions.
- Where consent is collected and used by a third party, the third party is to be named.
- Explicit consent (used for special category data) requires a very clear and specific statement.
- Individuals are to be told they can withdraw their consent at any time, how to withdraw their consent (this should be clear and easy)
- Schools are to keep evidence of consent ie who was asked, when, how, what and the rationale for their consent.
- Consent is kept under review and refreshed if anything changes
- Consent is not to be a precondition of service.

Schools are to avoid over-reliance on consent, where it is required it is to be freely given and care taken to ensure that there is not an imbalance of power between the data subject and controller.

7.2 Limitation, minimisation and accuracy.

FCAT will only collect personal data for specified, explicit and legitimate reasons and will explain these reasons to individuals when the information if first gathered i.e. via a Privacy Notice.

Staff must only process personal data where if is necessary in order to carry out their job.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

Part 8: Sharing personal data

FCAT will not normally share personal data, but may do so where;

- There is an issue with a pupil or parent / carer that puts the safety of our staff at risk
- The Trust needs to liaise with other agencies – (we will consent as necessary)
- Suppliers or contractors need data to enable the Trust to provide services to staff and pupils (e.g. IT Companies). If they can provide sufficient guarantees that they comply with data protection law, establish a data sharing agreement.

FCAT will share personal data with law enforcement and government bodies where legally required to do so, including:

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

Personal data may also be shared with the emergency services and local authorities to help them respond to an emergency situation that affects any of our pupils and staff.

Where personal data us transferred to a country or territory outside the European Economic Area, it will do so in accordance with data protection law.

Part 9: Subject Access requests and other rights of individuals

9.1: Subject Access Requests: Individuals have a right to make a 'subject access request' to gain access to personal information held about them. This includes:

- Confirmation 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 of 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 us being applied to their data, and what the significance and consequences of this might be for the individual.

Subject access request must be submitted using the appropriate request form, either by letter or email to the school and the DPO informed.
School staff directly receiving a subject access request must immediately inform their SDC.

9.2 Children and Subject Access Requests. Personal data about a child belongs to that child and not the child's parents or carers. Children **below the age of 13** are generally not regarded to be mature enough to understand their rights and implications of a subject access request. Therefore, most subject access request from parents or carer of pupils may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to Subject Access Requests.
Schools are to:

- Ask individuals to prove their identification
- Contact the individual vie phone to confirm the request was made.
- Respond without delay and within 1 month of the receipt of the request
- Provide the information free of charge
- Inform and explain to individuals, where a request is complex or numerous, that the school requires an extension to the time limit and the information will be provided within 3 months from the original date of the request.

FCAT will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or other individual
- Would reveal the pupil is at risk of abuse, where the disclosure of that information would not be in the child's

best interest
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child.

If the request is unfounded or excessive, (e.g. repetitive or duplicate copies of information) FCAT may refuse to act on it, or charge a reasonable fee taking into account administrative costs. Individuals will be informed as to why the request has been refused and that they have a right to complain to the ICO.

9.4 Other data protection rights of the individual. In addition to subject access requests, individuals also have the right to:
- At any time, withdraw their consent to processing
- Ask FCAT to rectify, erase or restrict processing of their personal data, or object to the process of it
- Prevent the use of their personal data for direct marketing
- Challenge processing, which has been justified based on 'public interest'
- Request a copy of agreements under which personal data is transferred outside of the European Economic Area.
- Object to decisions based solely on automated decision making or profiling
- 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 their request using the appropriate request form, either by letter or email to the school and the DPO informed.
School staff directly receiving a subject access request must immediately inform their SDC.

Part 10: Parental requests to see educational records
As an academy, parents or those with parental responsibility, do not have a legal right to have access to their child's educational record (which includes most information about a pupil). However, in the interests of transparency FCAT, at its discretion, chooses to follow regulation 5 of the Educational Regulations 2005, which gives parents rights of access to their child's educational record.
Schools are to provide the information, free of charge, within 15 school days of receipt of a written request.

Part 11: CCTV
FCAT are able to use CCTV at various sites for safety and adheres to the ICO's code of practice for the use of CCTV. The Trust does not need to ask individuals' permission to use CCTV, but it is made clear at the relevant school sites that individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signage explaining CCTV is in use.
Enquiries about any CCTV systems should be directed to the SDC.

Part 12: Photographs and videos
As part of the Trust's activities, schools may take photographs and record images of individuals for safety and management purposes.
Schools are to obtain written consent from parents / carers for photographs and videos taken of their child for communication, marketing and promotional materials, including whole class photographs.
Where schools need consent, they will clearly explain how the photograph and /or video will be used to both the parent and child. This may include:
- Within school on notice boards and in school newsletters
- Outside of school by external agencies such as the school photographer and newspapers.

- Online on our school websites or social media pages.

Consent can be refused or withdrawn at any time. If consent is withdrawn, schools are to delete the photograph or video and not distribute it further.
When using photographs and videos in this way schools will not include any other personal information about the child, to ensure they cannot be identified.

Part 13: Data protection by design and default
FCAT has measures in place to demonstrate that data protection has been integrated into data processing activities, including:

- The appointment of a DPO
- Integrating data protection into internal documents and related policies.
- Providing regular training opportunities for staff
- Regularly conducting reviews and audits to test privacy measures and check compliance.
- Maintaining records of our processing activities.

Part14: Data security and storage of records
FCAT 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:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal are kept secured when not in use.
- Papers containing confidential personal data are not left on office and classroom desks, on staffroom tables, pinned to notice boards or left anywhere where there is general access.
- Where personal information needs to be taken off site, staff should sign it in an out from the school office.
- Password should comply with best practice, not shared, and updated on a regular basis.
- Portable devices such as USB sticks or external hard drives are not permitted regardless of encryption, as these pose additional risks to security.
- Staff and governors using devices that are not school owned, are expected to follow the same best practice regarding online security.
- Where personal data is shared with a third party, FCAT undertakes due diligence and reasonable steps to ensure it is stored securely and adequately protected.

Part 15: Disposal of records

Personal data that is no longer needed, is inaccurate or out of date and cannot or does not need to be rectified is to be disposed of securely.
Schools are to shred or incinerate paper-based records and overwrite or delete electronic files. When using third party organisations to safely dispose of records, schools are to obtain sufficient guarantees from their supplier to satisfy themselves that they are complying with data protection law.
Before disposing of documents schools are to check the Retention Schedule to confirm retention dates.

Part 16: Data Breaches

Schools are to make all reasonable endeavours to ensure personal data is protected and there are no data breaches.
In the unlikely event of a data breach or a suspected data breach, schools are to follow the procedure set out in Annex A.
When appropriate, the **DPO will report the data breach to the ICO within 72 hours.**

Part17: Training

All Directors, governors and staff should be provided with data protection training as part of their induction process.

Where changes to legislation, guidance or the school's processes make it necessary, data protection will form part of continuing professional development.

Part 18: Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated when there are changes to DPA 2018, guidance provided by case law or changes which will affect FCAT's practice.

Part 19: Links with other documents

- **Privacy notices for each data set**
- **Data breach register**
- **Data sets and Data register**
- **Retention Schedule**
- **Subject Request Forms**
- **Data Processor register – template for schools**
- **Suppression list – template for schools**