Saint Robert Lawrence Catholic Academy Trust

Data Protection Policy
Incorporating the provisions of the General Data Protection Regulation (GDPR)

This policy applies to all academies within Saint Robert Lawrence Catholic Academy Trust (The Trust) and is drawn up in compliance with the General Data Protection Regulation and Data Protection Act 2018 following advice and guidance published by the Information Commissioner's Office (ICO).

Definitions and explanations

The Information Commissioner's Office (ICO)
The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO has powers to fine bodies who are in breach of their obligations under the legislation. The Trust is required to register with the ICO and our registration number is: ZA221702 . Full details of our registration can be viewed at https://ico.org.uk/ESDWebPages/Entry/ZA221702.

The General Data Protection Regulation (GDPR) and the Data Protection Act
This is a European Directive which will become part of UK law in May 2018 in the Data Protection Act 2018 (which replaces the Data Protection Act 1998). The Data Protection Act 2018 (DPA) will remain in force after Brexit. For more details see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

The aim of the GDPR
The GDPR and the DPA exist to protect the data of individuals. They contain a series of safeguards for every individual built around the principles of privacy, confidentiality, respect and security. The GDPR is a response to the need to protect individual rights in an increasingly digital world.

Scope of the GDPR
It applies to everyone, including businesses, schools, academies and academy trusts. The Academy Trust is classed as a Public Body and as such has more obligations placed upon it than other organisations. The Trust has a mandatory obligation under the DPA to comply with the provisions of the GDPR.

What is classed as data under the GDPR and DPA?
Any information that relates to a living person that identifies them – their **Personal Data**. This can include, name, address, phone number, IP address, National Insurance Number for example.
Some data is considered to be more sensitive – an individual's **Sensitive Data.** This can include data relating to racial or ethinic origin, details about that person's opinions, political affiliation, religious or philosophical beliefs, trade union membership, health, sexual orientation, genetic or biometric data, Special Educational Needs and medical information for example, where any of these are processed in a way which could identify an individual.

What Data does the Academy Trust Collect?
The Trust collects and uses personal and sensitive data about staff and pupils, and will hold personal data about parents and other individuals who come into contact with the Academy Trust. This

information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the Trust complies with its statutory obligations.

Privacy by Design and Privacy Impact Assessments
The requirement that privacy must be designed into the processing of personal data by default has always been a principle for data protection. It has now been brought to the fore in the new legislation. Organisations with technologies and processes that are likely to result in a high risk to the rights of the data subjects are required to carry out a Privacy Impact Assessment.

Data Subject
Someone whose details we keep on file (paper or electronic, in a formal file or elsewhere).

Data Controller
The body who has overall responsibility for how the organisation manages data. The Data Controller will delegate the day to day management of this to data processors on its behalf. For the academies within Saint Robert Lawrence the Academy Trust is the Data Controller.

Data Processor
This is the person or organisation that collects, uses, processes, accesses, amends and shares the data that the Data Controller has collected or has authorised to be collected. It can be an academy, a member of staff, a third party company, a governor, a contractor or a temporary employee. It can also be another organisation such as the police or the Local Authority.

Data Protection Officer
The person appointed by the Data Controller to advise the Data Controller about its statutory obligations under the GDPR and DPA, to monitor compliance against those obligations, to provide advice about the data protection impact assessment, to be the point of contact for Data Subjects, to manage breach procedures, to advise on training. The Data Protection Officer for the Academy Trust is:
John Walker: john@jawalker.co.uk

Data Protection Policy

1. The Principles
This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the DPA and GDPR, and other related legislation. It will apply to data regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically. All staff in the Trust will be made aware of the importance of safeguarding data and those involved with the collection, processing, sharing and disclosure of personal and sensitive data will receive specific training so that they can carry out their duties and responsibilities in compliance with the guidelines in this policy. The Trust will adopt the principle of Privacy by Design in all its activities and will comply with the six principles of GDPR.

i. ***Personal data shall be processed lawfully, fairly and in a transparent manner:***
We must have a legitimate reason to hold the data. We explain this in the Privacy Notices published on our website and attached at Appendix 1a and 1b. Where we need to we will ask for consent to use or share data for a particular purpose. If you wish to withdraw consent then we

have a form for you to complete to allow us to process your request. This is published on our website and attached at Appendix 2. There are situations when you cannot withdraw consent and these are explained in Data Subject Rights at 2. below.

ii. ***Personal data shall be obtained only for one or more specified and lawful purposes:*** This means that we must not use data for any other purposes other than those originally given and that we must state the purpose when we collect the data. 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 and is allowable.

iii. ***Personal data shall be adequate, relevant and not excessive:*** We will collect the minimum amount of data needed for a particular task or reason. This ensures that in the unlikely event of there being a breach or a hack then only limited data can be lost.

iv. ***Personal data shall be accurate and where necessary, rectified and kept up to date:*** We collect data when pupils join the Trust and we will keep this up to date annually. If an individual feels that the information held is inaccurate, should no longer be held by the Trust or should not have been held by the Trust then a request should be made in writing to the Data Protection Officer who will investigate and confirm the action that has been taken.

v. ***Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose:*** The Trust has a Records Retention Policy and schedule which is published on each academy website and data will be stored in line with that schedule.

vi. ***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:*** We have processes in place to keep data safe. This includes paper files and electronic records. Our Information Security Procedures are attached at Appendix 3.

2. Data Subjects' Rights

Individuals have a right:

- to be informed
- of access to data stored about them or their children
- to rectification if there is an error on the data stored
- to erasure if there is no longer a need for school to keep the data
- to restrict processing, ie to limit what is done with their data
- to object to data being shared or collected

There may be occasions when Data Subjects are also themselves the subject of child protection and safeguarding concerns and we may share their data for the prevention and detection of crime. The Academy Trust will have a duty to share data in these circumstances in addition to sharing information with organisations such as the Department for Education, the Catholic Education Service, Social Care,

the Local Authority, and HMRC, amongst others. In some cases these obligations override data subject rights.

3. Subject Access Request

You can ask for copies of information that we hold about you or a pupil who you have parental responsibility for at the Trust. This is referred to as a Subject Access Request and we have provided a form and guidance on how you should do this at Appendix 4.

4. Processing Data

The Trust must have a legitimate reason to collect and process data about an individual and must process it lawfully. The Trust will collection and process data with regard to the following conditions:

i. ***The legal basis*** and authority we rely on for collecting and processing data in the Trust are:
   - consent has been gained from the data subject or their parent
   - performance of a contract where the data subject is a party
   - compliance with the Trust's legal obligations
   - to protect the vital interests of the data subject or other associated person
   - to carry out the processing that is in the public interest and/or official authority
   - it is necessary for the legitimate interests of the Data Controller or third party
   - in according with national law

ii. In addition any special (sensitive) categories of personal data will be processed on the grounds of:
   - explicit consent has been granted from the data subject or their parent
   - it is necessary to comply with employment rights or obligations
   - protection of the vital interests of the data subject or associated person
   - being necessary to comply with the legitimate interests of the Trust
   - existing personal data that has been made public by the data subject and is no longer confidential
   - bringing or defending legal claims
   - Child Protection and Safeguarding
   - national laws relating to the processing of genetic, biometric or health data

iii. ***Data sharing*** will only be done within the limits set by the GDPR. The Trust is obliged to follow guidance and instructions from the Nottingham Roman Catholic Education Service, the Catholic Education Service, Department for Education, the Education, Skills and Funding Agency, Companies House, the NHS, the Police, the Local Authority and other specialist organisations and will share information where it is required to do so. The basis for sharing or not sharing data are recorded by the Trust.

iv. ***Breaches and Non Compliance*** will be handled in accordance with the procedures set out in Appendix 5. The Trust expects that breaches will be rare as protecting and maintaining data subjects' rights is the purpose of this policy. However we will be open and transparent in identifying and reporting breaches to the relevant authorities and data subjects.

v. ***Consent*:** The Trust will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required. However in most cases data will only be processed if explicit consent has been obtained. Consent is defined by the GDPR as "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 affirmation action, signifies agreement to the processing of personal data relating to him or her". We may seek consent from young people also, and this will be dependent on the child's age and capacity and the reason for processing.

On the website we have 'Privacy Notices' that explain how data is collected and used. It is important to read those notices as it explains how data is used in detail.

On arrival at one of the academies in the Trust you will be asked to complete a form giving next of kin details, emergency contact and other essential information. We will also ask you to give consent to use the information for other relevant Trust purposes, as set out on the Data Collection Consent form.

Obtaining clear consent and ensuring that the consent remains in place is important for the Trust. We also want to ensure the accuracy of the information that we collect so we check the accuracy of the data we hold by asking you to update the Data Collection and Consent form annually to let us know whether your details or your decision about consent changes.

vi. ***Withdrawing Consent***: Consent can be withdrawn subject to contractual, statutory or regulatory constaints, Where more than one person has the ability to provide or withdraw consent the Trust will consider each situation on its merits and within the principles of GDPR and also child welfare, protection and safeguarding principles. We have provided a form for you to withdraw consent and this is at Appendix 2.

vii. ***Physical Security***: In each academy every secure area has individuals who are responsible for ensuring that the space is securely maintained and controlled if unoccupied, ie locked. Offices and cupboards that contain personal data will be secured if the processor is not present. The Business Manager/Premises Manager/ICT Manager/ is responsible for authorising access to secure areas under the instruction of the Headteacher. All staff, contractors and third parties who have access to lockable areas must take due care to prevent data breaches.

viii. ***Electronic Security***: The Trust takes appropriate measures to ensure that electronic data is password protected, encrypted and that permissions are granted only in so far as they are necessary to perform the task and no more. The Trust will ensure that *"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against the accidental loss or destruction of, or damage to, personal data."*

5. Secure Disposal of Data

Whenever data is destroyed or disposed of the Trust will ensure that this is carried out in compliance with the GDPR. Documents will be held in the secure archive pending destruction

which will be in line with the retention schedule. Paper copies will be disposed of using an approved and compliant contractor. The destruction of electronic data will be overseen by the school's appointed technician using approved and compliant organisations.
The destruction of memory sticks, hard drives, PCs, laptops and other electronic devices will be under the direction of the school's appointed technician.

6. Third Parties

A written agreement will be in place between the third party data processor and the Trust to confirm compliance with the GDPR principles and obligations to assist the Trust in the event of a data breach or subject access request, or enquiries from the ICO.

7. Training for staff, governors and directors

All existing staff will be trained under the new guidelines. All staff will be required to sign to say that they understand the principles of GDPR and their role in protecting data. New staff will be required to undertake training as part of induction. Refresher training will be provided annually. The Trust's Codes of Conduct and Disciplinary Policies will be updated to include specific references to everyone's responsibilities under the GDPR. Existing governors and directors will be trained on their role as Data Controllers and Data Processors under the new guidelines. New governors and directors will receive training as part of induction.

8. Complaints

If you have a concern about how your data has been collected, used, held or processed by the Trust then please refer to the Trust Complaints Procedure in the first instance which is available on each academy website. You have a right to complain if you feel that data has been shared without consent or lawful authority, or if you have asked us to erase, rectify, not process data and we have not agreed to your request. We will always seek to resolve issues on an informal basis, and then through our formal complaints procedure. If you have not been able to resolve your complaint informally then please complete the form contained in the Complaints Policy and we will contact you with more details about the timescale and process.

In the UK it is the ICO who has responsibility for enforcing the DPA obligations and their contact details can be found at www.ico.org.uk Helpline: 0303 123 1113 Email: casework@ico.org.uk

9. Policy Review

A review of the effectiveness of the Trust's GDPR compliance and processes will be conducted by the Data Protection Officer every 12 – 24 months and reported to the Trust Board.

The Data Protection Officer for the Academy Trust is:
John Walker: john@jawalker.co.uk

Appendix 1a

Saint Robert Lawrence Catholic Academy Trust
PRIVACY NOTICE – PUPILS

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number, unique learner number and address, email address)
- Parental Contact details
- Characteristics (such as ethnicity, language, religion, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information
- Relevant medical information
- Special Educational Needs information
- Information about behaviour incidents, exclusions
- Post 16 destinations
- School history
- Biometric information

The Trust also uses various third party tools to make sure that pupils' best interests are advanced. This includes financial software to manage budgets, which may include some pupil data. We use systems to take electronic payments for school meals and other payments. We use software to track progress and attainment.

Why we collect and use this information
We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services and benchmark ourselves with other providers
- to comply with the law regarding data sharing
- to fulfil our statutory functions as an Academy Trust and provider of education
- to verify identity for the services we provide, eg the use of biometric data for cashless catering
- we must keep up to date information about parents and carers for emergency contacts
- we also use contact information to keep pupils, parents, carers up to date about school event
- to protect and safeguard pupils
- to protect our property and assets and to detect and prevent crime

The lawful basis on which we use this information
The lawful basis for the Trust to collect information comes from a variety of sources, such as the Education Act 1996, Regulation 5 of The Education (Information About Individual Pupils) (England)

Regulations 2013, Article 6 and Article 9 of the GDPR. The Department for Education and Local Authorities require us to collect certain information and report back to them. This is called a 'public task' and is recognised in law as it is necessary to provide the information.

All Catholic Schools, Academies and Academy Trusts are governed under Canon Law and the Catholic Education Service has a lawful basis to collect, hold and process data for all Catholic schools, academies and academy trusts.

We also have obligations to collect data about children who are at risk of suffering harm, and to share that with other agencies who have a responsibility to safeguard children, such as the police and social care.

We will also share information with law enforcement agencies to assist with crime detection or prevention or where we may suspect a wrong doing which may result in criminal proceedings.

We also share information about pupils who may need or have an Education Health and Care Plan (or Statement of Special Educational Needs). Medical teams have access to some information about pupils, either by agreement or because the law says we must share that information, for example school nurses and health professionals may visit the Trust. Counselling services, careers services, occupational therapists are the type of people we will share information with, so long as we have consent or are required by law to do so.

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data
We hold pupil data in line with our Records Retention Schedule which is available on each academy website.

Who we share pupil information with
We routinely share pupil information with:

- schools/colleges/universities and other establishments that the pupils attend after leaving us
- our local authorities
- the Catholic Education Service
- the Nottingham Roman Catholic Diocesan Education Service
- the Department for Education (DfE)
- the academies within the Trust
- medical and health professionals
- multi agency teams and those organisations involved in child protection and safeguarding
- law enforcement agencies

Why we share pupil information
We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins The Trust's funding and educational attainment policy and monitoring.

We are required to share information about our pupils with the (DfE) under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements
To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The National Pupil Database (NPD)
The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013. To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data. For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:
https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data
Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, please refer to the academy website and complete the form Subject Access Request.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. If you are not satisfied that your concern has been resolved then please refer to the Trust's Complaints Procedure which is available on the academy website. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact
If you would like to discuss anything in this privacy notice, please contact our Data Protection Officer:

The Data Protection Officer for the Academy Trust is:
John Walker: john@jawalker.co.uk

Appendix 1b

Saint Robert Lawrence Catholic Academy Trust
PRIVACY NOTICE – STAFF

The categories of school workforce information that we collect, process, hold and share include

- personal information (such as name, address, email address, employee or teacher number, national insurance number)
- special categories of data (such as gender, age, ethnic group, marital status, religion, next of kin, trade union membership, membership of professional associations)
- contract information (such as start dates, hours worked, post, roles and salary information, employment history)
- work absence information (such as number of absences and reasons)
- medical details
- qualifications (and, where relevant, subjects taught)
- pre-employment checks (such as right to work in UK, information provided on job application forms)
- data connected to Disclosure and Barring including disqualification by association
- data required for the purposes of TUPE

Why we collect and use this information

We use school workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- support career development and succession planning
- enable individuals to be paid accurately taking account of their entitlements and deductions
- enable accurate records to be maintained relating to employer's pension schemes
- keep in contact with staff
- take appropriate action in the event of a critical incident
- staff welfare and support with disability
- complete statutory data collection returns to DfE
- improve financial modelling and planning
- enable ethnicity and disability monitoring
- supporting the work of the School Teachers' Review Body
- comply with guidance such as 'Working Together' and safeguarding obligations
- to protect our property and assets and to detect and prevent crime

If we are required to comply with other legal obligations not listed above we will share data only when it is lawful to do so.

The lawful basis on which we process this information

The lawful basis for the Trust to collect and process staff information comes from a variety of sources, such as the Article 6 and Article 9 of the GDPR, the Safeguarding of Vulnerable Groups Act 2006, the "Transfer of Undertakings (Protection of Employment) Regulations 2006" as amended by the "Collective Redundancies and Transfer of Undertakings (Protection of Employment) (Amendment) Regulations 2014 We also have obligations to organisations such as HMRC and the Department of Work and Pensions, the Department for Education and the Education Skills and Funding Agency under the terms of our Funding Agreement and Articles of Association.

All Catholic Schools, Academies and Academy Trusts are governed under Canon Law and the Catholic Education Service has a lawful basis to collect, hold and process data for all Catholic schools, academies and academy trusts.

The Department for Education collects data annually as part of the national school workforce census. https://www.gov.uk/education/data-collection-and-censuses-for-schools

Collecting this information
Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

Storing this information
We hold school workforce data in line with our Records Retention Policy and Schedule which is available on each academy website.

Who we share this information with
We routinely share this information with:

- our local authorities
- Nottingham Roman Catholic Diocesan Education Service
- The Catholic Education Service
- the Department for Education (DfE)
- our payroll providers
- our Human Resource Advisory and transactional services
- HMRC
- Our pensions administrators
- Law enforcement agencies

Why we share school workforce information
We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

Local authority
We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education (DfE)
We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.
We are required to share information about our pupils with the (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Data collection requirements
The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a

statutory return under sections 113 and 114 of the Education Act 2005
To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data. For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data
To contact the department: https://www.gov.uk/contact-dfe

Requesting access to your personal data
Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, please refer to the academy website and complete the form Subject Access Request.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. If you are not satisfied that your concern has been resolved then please refer to the Trust's Complaints Procedure which is available on the academy website. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact our Data Protection Officer:
The Data Protection Officer for the Academy Trust is:
John Walker: john@jawalker.co.uk

Appendix 2a

Saint Robert Lawrence Catholic Academy Trust
Withdrawal of Consent Form – on behalf of pupil

Please complete and sign this form and deliver to the academy office.

Please note that as a Trust we may have contractual, statutory and/or regulatory reasons why we will still process and hold details of a pupil, parent, staff member, volunteer or other person.

Where two parents share parental responsibility, or where parental responsibility is shared and the pupil is capable of expressing a view and there is conflict between the individuals, the process of withdrawing consent will be subject to an evaluation and discussion to enable a decision to be reached that is considered to be in the pupil's best interests.

We may need to seek identification evidence and have sight of any Court Order or Parental Responsibility Agreement in some cases to action this request. If this is the case a senior member of the academy staff will discuss this with you.

I withdraw consent for the Trust to process the personal data described below relating to the named pupil.

Name of person withdrawing consent	
Name of pupil that this withdrawal concerns	
A description of the personal data that this withdrawal concerns and for which consent was previously granted	
I confirm that I am the parent or carer of the named pupil and that I have parental responsibility for the pupil	*Signed:* *Date:*

For academy use only:	
Date received by academy	
Name of staff member receiving withdrawal form	
Record of actions taken	

Appendix 2b

Saint Robert Lawrence Catholic Academy Trust
Withdrawal of Consent Form – Adult

Please complete and sign this form and deliver to the academy office.

Please note that as a Trust we may have contractual, statutory and/or regulatory reasons why we will still process and hold details of a pupil, parent, staff member, volunteer or other person.

I withdraw consent for the Trust to process the personal data described below for which consent was previously granted.

Name of person withdrawing consent	
A description of the personal data that this withdrawal concerns for which consent was previously granted	
Signed: *Date:*	

For academy use only:	
Date received by academy	
Name of staff member receiving withdrawal form	
Record of actions taken	

Appendix 3

Saint Robert Lawrence Catholic Academy Trust

Information Security Procedures

The Trust reserves the right to monitor the use of ICT systems and information including email and internet usage, to protect the confidentiality, integrity and availability of the Trust's information assets and ensure compliance with Trust policies.

The Trust has the following procedures in place to safeguard information.

Access Control	Staff are allocated permissions on the network relevant to their job role, status, expertise and authority. Access to paper copies is restricted to those whose job involves the legitimate processing of that data.
Encryption and Cryptographic controls	The Trust has instigated system wide controls which prevent the use of non-encrypted devices gaining access to the network. The Trust has instigated policies which prohibit the use of own devices which are not encrypted. Staff have received training and an advice leaflet.
ICT , internet and Email Acceptable Use	Staff and pupils are issued with an Acceptable Use Policy and Codes of Conduct which all are required to accept and sign. Failure to comply with these codes is a disciplinary offence. Staff are reminded regularly through staff briefing. Students are reminded as part of the ICT curriculum.
Data Backup and Recovery	The Trust has procedures in place to ensure its network and the data contained on it is backed up and that the backups are available to restore in the event of a critical incident. The Trust obtains from third party data processors assurances that they also have robust back up procedures in place.
Password Protection	The Trust has a password policy in place which is built in to the ICT system and requires all users to set a secure password which must be changed regularly. Staff have been given guidance on how to password protect documents.
Secure Email	All staff know to use only the academy email addresses for academy and Trust business. Staff have been issued with guidance on how to encrypt emails.
Secure File Transfer	The Trust uses the recommended Common Transfer File and Admissions Transfer File to send and receive pupil data between schools and between the Trust and the Local Authority.
Records Retention and Disposal	The Trust has a Records Retention Schedule in place which lists all types of data and information. The Trust archive is maintained and documents are retrieved for confidential and secure disposal annually.
Public Internet Access – guest WiFi	The Trust provides a guest WiFi connection which allows access to the internet without access to any of the Academy Trust systems.
Business Continuity	The Trust has in place a Business Continuity Management Plan which includes an ICT Disaster Recovery Plan which is tested for

	effectiveness annually.
Third Party Data Processors	The Trust has issued a letter to each third party data processor to seek assurances that the data processor is compliant with GDPR. All new suppliers and data processors will need to complete a declaration.

Appendix 4

Saint Robert Lawrence Catholic Academy Trust

Procedures for responding to Subject Access Requests made under the Data Protection Act 2018 and General Data Protection Regulation

Rights of access to information

There are two distinct rights of access to information held by schools about individuals:

1. Under the Data Protection Act 2018 and GDPR any individual has the right to make a request to access the personal information held about them.

2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (Wales) Regulations 2004.

Actioning a subject access request

1. Requests for information must be made in writing and we have provided a form for this purpose: "Subject Access Request Form" which can be sent by email addressed to the Data Protection Officer. If the initial request does not clearly identify the information required, then further enquiries will be made to establish the information required.

2. The identity of the requestor must be established before the disclosure of any information, and checks will be carried out regarding proof of relationship to the child if a request is being made by a parent. Evidence of identity can be established by requesting a combination of the following documents:

- passport
- driving licence
- utility bills with the current address
- birth/ marriage certificate
- P45/P60
- credit card or mortgage statement *This list is not exhaustive – please see Subject Access Request Form*

3. Any individual has the right of access to information held about themselves. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. Personal data about a child belongs to that child. The Trust will obtain the permission of the child if appropriate prior to disclosure of information. The Trust will decide on a case-by-case basis whether to grant such requests, bearing in mind guidance issued from time to time from the Information Commissioner's Office.

4. The school may make a charge for the provision of information, dependent upon the following:

- Should the information requested contain the educational record then the amount charged will be dependent upon the number of pages provided.
- Should the information requested be personal information that does not include any information contained within educational records schools can charge up to £10 to provide it.
- If the information requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Trust.

5. The response time for subject access requests for all or part of the pupil's educational record, once officially received, is 15 school days. If the subject access request does not relate to the educational

record, we will respond within one month. However the one month will not commence until after receipt of fees or clarification of information sought.

6. The Data Protection Act 2018 allows exemptions regarding the provision of some information; therefore all information will be reviewed prior to disclosure.

7. Third party information is that which has been provided by another body, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent will normally be obtained. The 40 day statutory timescale will still apply.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another individual may not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings be disclosed.

9. If there are concerns over the disclosure of information then additional advice should be sought.

10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

12. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

Safeguarding

The Academy Trust's responsibilities in relation to Child Protection and Safeguarding will always be considered and where there is any doubt about whether or not to disclose information then Safeguarding priorities will take precedence over data protection and subject access requests.

Complaints

Complaints about the above procedures should be referred to the Academy Trust Complaints Co-ordinator who will decide whether it is appropriate for the complaint to be dealt with in accordance with the Trust's Complaints Procedure. Complaints which are considered outside of the scope of the Academy Trust's Complaint Procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Contacts

If you have any queries or concerns regarding this procedure then please contact the Data Protection Officer. Contact details are available on request.

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk or telephone 0303 123 1113.

Saint Robert Lawrence Catholic Academy Trust

SUBJECT ACCESS REQUEST FORM

Please complete this form if you want us to supply you with a copy of any personal data we hold about you. You are entitled to receive this information under the Data Protection Act 2018 (DPA) and the EU General Data Protection Regulation (GDPR), which comes into effect on 25 May 2018. We will also provide you with information about any processing of your personal data that is being carried out, the retention periods which apply to your personal data, and any rights to rectification, erasure, or restriction of processing that may exist.

We will endeavour to respond promptly and in any event within one month of the latest of the following:

- Our receipt of your written request; or
- Our receipt of any further information we may ask you to provide to enable us to comply with your request.

The information you supply in this form will only be used for the purposes of identifying the personal data you are requesting and responding to your request. You are not obliged to complete this form to make a request, but doing so will make it easier for us to process your request quickly.

1) Details of the person requesting information

Full Name:

Address (including postcode):

Contact Telephone Number:

Contact Email Address:

To ensure we are releasing data to the right person we require you to provide us with proof of your identity and of your address. If we are not satisfied you are who you claim to be, we reserve the right to refuse to grant your request.

Please supply us with a photocopy or scanned image (do not send the originals) of one of ***both*** of the following:

a) Proof of Identity Passport, photo driving licence, national identity card, birth certificate.

b) Proof of Address Utility bill, bank statement, credit card statement (no more than 3 months old); current driving licence; current TV licence; local authority tax bill, HMRC tax document (no more than 1 year old). Alternatively, you can post this proof of identification to the Academy Trust.

2) What information are you seeking?

Please describe the information you are seeking. Please provide any relevant details you think will help us to identify the information you require. Please note that if the information you request reveals details directly or indirectly about another person we will have to seek the consent of that person before we can let you see that information. In certain circumstances, where disclosure would adversely affect the rights and freedoms of others, we may not be able to disclose the information to you, in which case you will be informed promptly and given full reasons for that decision. While in most cases we will be happy to provide you with copies of the information you request, we nevertheless reserve the right, in accordance with Article 12 of the GDPR to charge a fee or refuse the request if it is considered to be "manifestly unfounded or excessive". However we will make every effort to provide you with a satisfactory form of access or summary of information if suitable.

3) Information about the collection and processing of data

If you want information about any of the following, please tick the boxes:

- ☐ Why we are processing your personal data
- ☐ To whom your personal data are disclosed
- ☐ The source of your personal data

4) Declaration

I confirm that I have read and understood the terms of this subject access form and certify that the information given in this application is true. I understand that it is necessary for the Trust to verify my

identity and it may be necessary to obtain more detailed information in order to locate the correct personal data.

Signed: Date:

Appendix 5

Saint Robert Lawrence Catholic Academy Trust
Data Breach Procedures

This procedure is designed to ensure that all staff, governors and directors are aware of what to do in the event of a DPA / GDPR breach and that they need to act swiftly to report the breach. The attached 'Data Breach Flowchart' outlines the process.

The Trust recognises that most breaches, aside from cyber criminal attacks, occur as a result of human error. They are not malicious in origin and if quickly reported are often manageable.

Examples of breaches are:-

- Information being posted to an incorrect address which results in an unintended recipient reading that information
- Loss of mobile or portable data device, unencrypted mobile phone, laptop, USB memory stick or similar
- Sending an email with personal data to the wrong person or to too many people who may not need to or be entitled to see the data
- Dropping or leaving documents containing personal data in a public place
- Personal data being left unattended at a printer enabling unauthorised persons to read that information
- Not securing documents containing personal data (at home or work) when left unattended
- Anything that enables an unauthorised individual access to school buildings or computer systems
- Discussing personal data with someone not entitled to it, either by phone or in person. How can you be sure they are entitled to that information?
- Deliberately accessing, or attempting to access or use personal data beyond the requirements of an individual's job role e.g. for personal, commercial or political use. This action may constitute a criminal offence under the Computer Misuse Act as well as the Data Protection Act.
- Opening a malicious email attachment or clicking on a link from an external or unfamiliar source, which leads to the Trust's equipment (and subsequently its records) being subjected to a virus or malicious attack, which results in unauthorised access to, loss, destruction or damage to personal data.

What should staff do?

Being open about the possible breach and explaining what has been lost or potentially accessed is an important element of working with the ICO to mitigate the impact. Covering up a breach is never acceptable and may be a criminal, civil or disciplinary matter. Report the breach to the Data Controller and Data Protection Officer as soon as possible, this is essential.

What will happen next?

The breach notification form will be completed and the breach register updated. The breach report to the ICO will be submitted within 72 hours of the Data Controller becoming aware of the breach.

If the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach notification to those people will be done in a co-ordinated manner with support from the DPO.
It may not be possible to investigate the breach fully within the 72 hour timeframe. Information about further investigations will be shared with the ICO with support from the DPO.

Breach notification to data subject
For every breach the Trust will consider notification to the data subject or subjects as part of the process. If the breach is likely to be high risk they will be notified as soon as possible and kept informed of actions and outcomes.

The breach and process will be described in clear and plain language.

If the breach affects a high volume of data subjects and personal data records, the most effective form of notification will be used and discussed with the Data Controller with support from the Data Protection Officer.

Advice will be taken from the ICO about how to manage communication with data subjects if appropriate.

A post breach action plan will be put into place and reviewed.

Evidence Collection
It may be necessary to collect information about how an information security breach or unauthorised release of data occurred. This evidence gathering process may be used as part of an internal process (which can include disciplinary proceedings), it may be a source of information for the ICO, it could also be used within criminal or civil proceedings.

This process will be conducted by a suitable member of the Trust, which may be the er or Data Protection Officer, but will be determined depending on the nature of the breach.

Guidance may be required from external legal providers and police may be involved to determine the best way to secure evidence.

A record of what evidence has been gathered, stored and secured must be available as a separate log. Files and hardware must be securely stored, possibly in a designated offsite facility.

Evidence Collection Log

Date	Evidence Description	Secure storage location & confirmed date	Trust Officer

Data Breach Notification Form

When did the breach occur (or become known)?	
Who was involved in the Trust?	
Who was this reported to?	
Date and time it was reported	
Date and time DPO notified	
A description of the nature of the breach. This must include the type of information that was lost, e.g. name, address, medical information, NI numbers	
The categories of personal data affected – electronic, hard copy	
Approximate number of data subjects affected.	
Approximate number of personal data records affected.	
Name and contact details of the Data Protection Officer / GDPR Owner.	
Consequences of the breach. What are the potential risks?	
Any measures taken to address the breach. What actions and timeline have been identified?	
Any information relating to the data breach.	

Breach Management Flowchart