Data Protection Policy

(Statutory Policy)

Created by: Miss C Huddleston

Date presented to Governors: 03 October 2019
Review Date: Autumn Term 2020

For public viewing

Link to other policies and documents:

- Data Protection Policy
- Data Security Policy
- Data Retention Policy
- Information and Records Management Society's: Toolkit for Schools
- CCTV Policy
- Charging and Remission Policy

Contents

1. Aims

St Wilfrid's Church of England Academy aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act (2018) (hereafter DPA 2018).

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

2. Scope

This policy applies to current and former employees, Governors, volunteers, apprentices and consultants. If you fall into one of these categories, then you are a 'data subject' for the purposes of this policy. Please read this policy alongside your contract of employment (or contract for services) and any other notice the Academy issues from time to time in relation to personal data.

The Academy has separate policies and privacy notices in place in respect of job applicants, students, parents and other categories of data subject. Copies can be obtained from the Office

The Academy has measures in place to protect the security of personal data in accordance with the Data Security Policy. A copy of the Data Security Policy can be obtained from the Office.

The Academy will hold data in accordance with its ***Data Retention Policy***. A copy can be obtained from the office. We will only hold data for as long as necessary for the purposes for which it was collected.

The Academy is a 'Data Controller' for the purposes of processing personal data. This means that the Academy determines the purpose and means of the processing of personal data.

This policy explains how the Academy will hold and process personal data. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, the Academy

3. Legislation and Guidance

This policy meets the requirements of the GDPR and 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 meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with our funding agreement and articles of association.

4. Definitions

Term	Definition
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 a username It may also include factors specific to the individual's physical, physiological, genetic, mental, 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, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual 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.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes 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 personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

5. The Data Controller

The Academy processes personal data relating to parents, students, staff, governors, visitors and others, and therefore is a data controller.

The Academy is registered as a data controller with the ICO – registration number Z3050817 and will renew this registration annually or as otherwise legally required.

The Academy delegates the responsibility of the Data Controller to the Data Controllers Representative (See Section 6 below).

6. Roles and Responsibilities

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

Governing Board

The governing board has overall responsibility for ensuring that our Academy complies with all relevant data protection obligations.

Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on Academy data protection issues.

The DPO is also the first point of contact for individuals whose data the Academy processes, and for the ICO.

Full details of the DPO's responsibilities are set out in the service level agreement.

Our DPO is The Schools People (see Contact details – Section 23, below)

Principal

The Principal acts as the Data Controller's representation on a day-to-day basis.

All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Academy of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
- 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
- Prior to 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

7. Data Protection Principles

The GDPR is based on data protection principles that the Academy must comply with. The principles say that 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, 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 the Academy aims to comply with these principles.

8. Lawful Bases for Processing Personal Data

Lawfulness, Fairness and Transparency

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

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

The Academy can process personal data for these purposes without knowledge or consent.
The Academy will not use personal data for an unrelated purpose without disclosing the intent and providing the legal basis for the processing.

Where the student is under 13 years of age, we will seek written consent from the parent/carer, and they will be advised of their right to withdraw that consent at any time (except for online counselling and preventive services).

Whenever we first collect personal data from individuals, we will provide them with the relevant information including details of the data we collect and how it is collected, stored and shared, via a Privacy Notice (sometimes called a Fair Processing Notice) as required by the GDPR and the Data Protection Act 2018

Special Category Data

In processing 'special categories' of personal data, we will also meet one of the special category conditions set out in the GDPR and Data Protection Act 2018.

- The individual or person with the lawful authority to exercise consent on individual has given explicit consent;
- The data needs to be processes to ensure the vital interest of the individual where they are physically or legally incapable of giving consent;
- The data has manifestly made public by the individual e.g. on social media
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

Criminal Convictions

The Academy may use information relating to criminal convictions where the law allows us to do so. It is envisaged the Academy will hold information about criminal convictions if information about criminal convictions comes to light as a result of our recruitment and Disclosure and Barring Service checks, or if information about criminal convictions comes to light during employment with us. Information about criminal convictions and offences will be used in the following ways:

- To ensure employee suitability to work
- For safeguarding purposes

Less commonly, information relating to criminal convictions may be used where necessary in relation to legal claims; where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

If we offer online services to students, such as classroom apps, and we intend to rely solely on consent as a basis for processing, written consent will be obtained directly from the students and they will be advised of their right to withdraw consent for the processing at any time.

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.

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 to further processing where necessary.

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

When staff no longer need the personal data they hold, they must ensure it is stored, deleted or anonymised in accordance with the Information and Records Management Society's Toolkit for Schools.

Examples of When the Academy Might Process Personal Data

The Academy must process personal data in various situations during recruitment, employment (or engagement) and even following termination of employment (or engagement). For example:

- Making a decision about your recruitment or appointment;
- Determining the terms on which you work for us;
- Checking you are legally entitled to work in the UK;
- Checking the award of Qualified Teacher Status, completion of teacher induction and prohibitions, sanctions and restrictions that might prevent the individual from taking part in certain activities or working;
- To maintain our single central record and to comply with our general safeguarding obligations;
- To provide information on our website about our employees;
- Paying you and, if you are an employee, deducting tax and National Insurance contributions;
- Liaising with your pension provider;
- Administering the contract entered into with you;
- In order to operate as an Academy, which may involve us sharing certain information about our staff with our stakeholders or processing correspondence or other documents, audits or reports which contain your personal data;
- Business management and planning, including accounting and auditing
- Conducting performance reviews, managing performance and determining performance requirements;
- Making decisions about salary reviews and compensation;
- Assessing qualifications for a particular job or task, including decisions about promotions;
- Gathering evidence for possible grievance or disciplinary hearings;
- Responding to complaints or investigations from stakeholders or our regulators;
- Making decisions about your continued employment or engagement;
- Making arrangements for the termination of our working relationship;
- Providing references to prospective employers;
- Education, training and development requirements;
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work;
- Ascertaining your fitness to work;

- Managing sickness absence;
- Complying with health and safety obligations;
- To prevent fraud;
- To monitor your use of our information and communication systems to ensure compliance with our IT policies;
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution;
- To conduct data analysis studies to review and better understand employee retention and attrition rates;
- In connection with the Transfer of Undertaking (Protection of Employment) Regulations 2006, for example, if a service is outsourced or in connection with an academy conversion.
- To maintain and promote equality in the workplace;
- To comply with requirements of the Blackburn Diocesan Board of Education to share personal data about employees to the extent that they require it to fulfil their functions
- To receive advice from external advisors and consultants;
- In appropriate circumstances to liaise with regulatory bodies, such as the NCTL, the Department for Education, the DBS and the Local Authority about your suitability to work in a school or in connection with other regulatory matters;
- for any other reason which the Academy is obliged to give notice of, from time to time.

9. Sharing Personal Data

The Academy is obliged to share your personal data in order to meet obligations under our contract with you, or to meet our statutory obligations, or for our legitimate interests. Examples of organisations with whom we share your personal data include, but are not limited to:

- Department for Education
- The Local Authority
- Ofsted
- Disclosure and Barring Service
- HMRC
- Teachers' Pension Service
- Local Government Pension Service

Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies, HR Consultants, Occupational Health Services etc. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with current data protection legislation
- 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 carryout 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, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- 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 students or staff.

Other instances where we may share personal data include:

- There is an issue with a student or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this

10. Transferring Data Outside The EEA

We do not routinely share data with organisations outside the EEA. Where this may be necessary, e.g. where a former employee has emigrated and/or applied to work outside the EEA, data may be transferred to the new employee with explicit consent from the former employee and with appropriate safeguards.

We will not transfer personal data outside the European Economic Area (EEA) unless such transfer complies with the GDPR. This means that we cannot transfer any personal data outside the EEA unless:

- The EU Commission has decided that another country or international organisation ensures an adequate level of protection for personal data
- One of the derogations in the GDPR applies (including if an individual explicitly consents to the proposed transfer).

11. How Personal Data Should be Processed on Behalf of the Academy

Everyone who works for, or on behalf of, the Academy has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Academy's Data Security and Data Retention policies.

The Academy's Data Protection Officer and the Data Controller's Representative are responsible for reviewing this policy and updating the Governing Body on the Academy's data protection responsibilities and any risks in relation to the processing of data. Any questions in relation to this policy or data protection should be directed to these persons.
Staff should only access personal data covered by this policy if it is required for the work they do for, or on behalf of the Academy and only if authorised to do so.

Staff should only use the data for the specified lawful purpose for which it was obtained.

Staff should not share personal data informally.

Staff should keep personal data secure and not share it with unauthorised people.

Staff should regularly review and update personal data which they have to deal with for work. This includes telling the Academy if their own contact details change.

Staff should not make unnecessary copies of personal data and should keep and dispose of any copies securely.

Staff should use strong passwords.

Staff should lock computer screens when not at their desks.

Personal data should be encrypted before being transferred electronically to authorised external contacts. Speak to IT for more information on how to do this.

Staff should not save personal data to their own computers or other electronic devices.

Personal data should never be transferred outside the European Economic Area except in compliance with GDPR and the Data Protection Act (2018) and in consultation with the Data Controllers representative and the DPO.

Staff should not leave paper containing personal data lying about on desks. Storage drawers and filing cabinets should be locked.

Staff should not take personal data away from Academy premises without authorisation from their line-manager.

Where possible paper copies of personal data should be shredded and disposed of securely following transfer to electronic systems. Where hard copy data is retained it should be done so securely.

Staff should ask for help from the Data Protection Officer/ if they are unsure about data protection or if they notice any areas of data protection or security that can improve upon.

Any deliberate or negligent breach of this policy may result in disciplinary action being taken in accordance with the Academy's Disciplinary Procedure.

It is a criminal offence to conceal or destroy personal data which is part of a Subject Access Request (see below). Such conduct would also amount to gross misconduct under the Academy's Disciplinary procedure and could result in dismissal.

12. Data Breaches

The Academy has robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur then the Academy must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals, then the Information Commissioner's Office must be notified within 72 hours.

If any staff member is aware of a Data Breach, they must contact their line manager immediately and keep any evidence they have in relation to the breach.

For further information please refer to the ***Data Security Policy and Breach Procedure***.

13. Subject Access Requests and Other Data Subject Rights

Subject Access Requests (SARs)

Individuals have a right to make a 'subject access request' to gain access to personal information that the Academy 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

A SAR may be made in writing or verbally, through traditional channels of communication or through Social Media. If a SAR request is received it should forward it immediately to the Data Controllers Representative who will liaise with the Data Protection Officer and coordinate a response.

A SAR ***does not*** have to contain the words Subject Access Request. Any communication, whether written or verbal, t**hat requests access to personal data should be treated as a possible SAR.** Refer to the ***Subject Access Request Policy and Procedure*** for further information.

A form is available to staff, Governors, and other stakeholders who work for or on behalf of the Academy who wish to make a SAR in relation to their own personal data. Use of the form is not compulsory. The Academy must accept a SAR in any written or verbal form. The Academy may however, contact the requester to for further information if necessary. At a minimum a SAR must contain:

- The requesters full legal name
- Correspondence address
- Contact number and email address
- Details of the information requested

Please refer to the ***Subject Access Request Policy and Procedure*** for further information

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 aged 12 and above are generally 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 students at our Academy may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by- case basis.

Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification if we are not confident about the requester's identity
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of a valid Subject Access Request. A request is not considered valid until we have confirmed the identity if the requester and their entitlement to the requested data
- 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 numerous. We will inform the individual of this within 1 month, 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 or another individual
- 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
- 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, we may refuse to act on it, or charge a reasonable fee which takes 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.

Other Data Protection Rights of the Individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time if consent is the sole basis for processing
- 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 Data Controllers Representative

14. Parental Requests to Education Records

There is no automatic parental right of access to the educational record in an Academy. However, written requests can be made via the PA to the Principal. A charge may apply in line with the ***Charging and Remission Policy***

15. CCTV

We use CCTV in various locations around the Academy site. We will adhere to the ICO's code of practice for the use of CCTV.

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

For more information about the Academy's use of CCTV please refer to ***CCTV Policy***

Any enquiries about the CCTV system should be directed to the Computer Services Team.

16. Photographs and Videos

As part of Academy activities, we may take photographs and record images of individuals within the Academy

Staff must not take images of children unless they have:

- A legitimate reason for doing so
- Permission to do so

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.
Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.
Uses may include:

- Within the Academy on notice boards and in Academy magazines, brochures, newsletters, etc.
- Outside of Academy by external agencies such as the Academy photographer, newspapers, campaigns
- Online on our Academy website or social media pages

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.

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.

17. 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 processing activities, including:

- 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 law (see section 6)
- Completing privacy impact assessments where the Academy's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting 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 Academy 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

18. 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:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- 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
- Where personal information needs to be taken off site, staff must sign it in and out from the Academy

office

- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Passwords that are at least 8 characters long containing letters and numbers are used to access Academy computers, laptops and other electronic devices. Staff and students are reminded to change their passwords at regular intervals
- Staff, students or Governors who store personal information on their personal devices are expected to follow the same security procedures as for Academy-owned equipment (see our Staff Information Systems Code of Conduct)
- 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 (see section 8)

19. Disposal of Records

Personal data that is no longer needed will be disposed of securely in accordance with our Data Retention Policy.

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 or incinerate paper-based records, and overwrite or delete electronic files.

We may also use a third-party to safely dispose of records on the Academy's behalf. If we do so, we will require the third-party to provide sufficient guarantees that it complies with current data protection law and provides a Certificate of Destruction for our records.

20. Personal Data Breaches

The Academy 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 our ***Data Security Policy and Breach Procedure***.
When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches may include, but are not limited to:

- A non-anonymised dataset being published on the Academy website which shows the exam results of students eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- Theft of an Academy laptop containing non-encrypted personal data about students

See the **Data Security Policy and Breach Procedure** for more information

21. Training

All staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Academy's processes make it necessary.

22. Monitoring Arrangements

The Data Controller's Representative, together with the Data Protection Officer are responsible for monitoring and reviewing this policy.

The Data Controller's Representative, together with the Data Protection Officer check that the Academy complies with this policy by, among other things, reviewing records, policies and procedures annually.

This policy will be reviewed and updated as and when necessary in relation to any amendments to Data Protection legislation or guidance, or any internal concerns resulting from policy violations, data breached, or on an annual basis.

At every review, the policy will be shared with the Governing Board.

23. Contacts

Questions or concerns about how the Academy process personal information or any requests to exercise data protection rights, should be submitted to the Academy in the first instance.

If the Academy is not able to address concerns and resolve them satisfactorily, please contact the Data Protection Officer at the address below.

Finally, concerns can be registered with the UK's data protection regulator, the Information Commissioner's Office, by following this link https://ico.org.uk/make-a-complaint/

Contact Details

Data Controller: St Wilfrid's C of E Academy, Duckworth Street, Blackburn, BB2 2JR

Data Controller's Representative: Cath Huddleston, Principal, Email: chuddleston@saintwilfrids.com

Data Protection Officer: Dee Whitmore. Email: dposervice@schoolspeople.co.uk

Telephone: 01773 851 078;

Postal Address: 44 Tyndall Court, Peterborough, Cambridgeshire, PE2 6LR.