

St. Ann's R.C. Primary School

Data Protection Policy

Last reviewed: October 2023
Next review by: October 2024

Our School's Mission Statement

'We, the family of St. Ann's, rejoice in our learning; striving for excellence. We challenge ourselves, follow Jesus and empower each other to be the best we can be.

Motivate, learn, inspire.'

Our Commitment

St Ann's R C Primary School is committed to protecting and respecting the confidentiality of sensitive information held in school relating to staff, pupils, parents and governors.

St Ann's R C Primary School needs to keep certain information about employees, pupils and other users to allow us, for example, to monitor performance, achievement and health and safety.

Personal pupil information held in school includes:

- Names of pupils.
- Dates of birth.
- Unique pupil number.
- Address.
- Ethnicity.
- Language.
- Nationality and country of birth.
- Free school meal eligibility.
- School marks.
- Medical information.
- Exam results.
- SEN assessments and data.
- Attendance information (sessions attended, number of absences and absence reasons)
- Exclusions and behavioural information.

Personal staff information held in school includes:

- Name.
- Date of birth.
- Address.
- Employee or teacher number.
- National Insurance number.
- Ethnicity.
- Contract information (including start dates, hours worked, post, roles and salary)
- Attendance information.
- Qualifications.
- Bank details

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, we must comply with the Data Protection Principles which are set out in the Data Protection Act (DPA).

<https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/>

Changes to data protection legislation (GDPR May 2018) shall be monitored and implemented in order to remain compliant with all requirements.

The members of staff responsible for data protection are Mrs Maria Noctor (Headteacher) and Liz Cooper and Tracy Bradbury (School Administrators)

The school is also committed to ensuring that its staff are aware of data protection policies, legal requirements and adequate training is provided to them.

The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school. All staff are made aware of the controls set out in this policy. Staff are trained initially at induction and training is refreshed at regular intervals at staff meetings and Key Stage meetings.

Notification

Our data processing activities will be registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller. Details are available from the ICO:

<https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/>

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

Breaches of personal or sensitive data shall be notified within 72 hours to the individual(s) concerned and the ICO.

Personal and Sensitive Data

All data within the school's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

The definitions of personal and sensitive data shall be as those published by the ICO for guidance:

<https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions>

The principles of the Data Protection Act shall be applied to all data processed:

- ensure that data is fairly and lawfully processed
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive
- ensure that data processed is accurate
- not keep data longer than is necessary
- process the data in accordance with the data subject's rights
- ensure that data is secure
- ensure that data is not transferred to other countries without adequate protection.

Responsibilities of Staff

All staff are responsible for:

- i. Checking that any information that they provide to the School in connection with their employment is accurate and up to date.
- ii. Informing the School of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The School cannot be held responsible for any errors unless the staff member has informed the School of such changes.

iii. Handling all personal data (eg – pupil attainment data) with reference to this policy.

Fair Processing / Privacy Notice

The school has a Privacy Notice in place for pupils and staff. (Appendix 1 and 2)

Data Security

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them.

Risk and impact assessments shall be conducted in accordance with guidance given by the ICO:

<https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/>

<https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2014/02/privacy-impact-assessments-code-published/>

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.

The security arrangements of any organisation with which data is shared shall also be considered and these organisations shall provide evidence of the competence in the security of shared data.

Data Access Requests

All individuals whose data is held by us, has a legal right to request access to such data or information about what is held and should be made in writing to:

Mrs Maria Noctor

St Ann's R C Primary School

Derbyshire Lane

Stretford

M32 8SH

No charge will be applied to process the request.

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. Data may be disclosed to the following third parties without consent:

- **Other schools**

If a pupil transfers from St Ann's R C Primary School to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.

- **Examination/assessment authorities**

This may be for registration purposes, to allow the pupils in school to sit Key stage 2 tests and phonic screening check and external moderation of teacher assessment

- **Health authorities**

As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

• **Police and courts**

If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

• **Social workers and support agencies**

In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

• **Educational division**

Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

• **Right to be Forgotten:**

Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the school including any data held by contracted processors.

Photographs and Video

Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in school and on the school's website. A parent has the opportunity to request that their child is not photographed.

It is the school's policy that external parties (including parents) may not capture images of staff or pupils during such activities without prior consent.

Location of information and data

Hard copy data, records, and personal information are stored out of sight and in a locked cupboard. The only exception to this is medical information that may require immediate access during the school day. This will be stored in the Infant and Junior office and should not be removed from the school site.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.
- Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
- If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.
- If it is necessary to transport data away from the school, it should be downloaded onto a USB stick. The data should not be transferred from this stick onto any home or public computers. Work should be edited from the USB, and saved onto the USB only.

- All teacher laptops are password protected with bitlocker (encryption) to ensure any data held on the laptops are safe should they be stolen or lost.
- The computers in the Infant and Junior offices are password protected. Each computer in the offices has a privacy filter on the screen to stop other people viewing confidential information. Office staff ensure that computers are locked whenever they are unattended.
- Ipads/Ipods are with file browser as linked to shared drive and are all password protected.
- The Shared Drive is hosted by the server, server has a password.

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

Data transfer methods

This section lists the main methods of data transfer and also sets out any restrictions and requirements for the secure transfer of controlled data.

Whenever the school transfers data a written contract needs to be in place. The contract is important so that both parties understand their responsibilities and liabilities. The school checks that the processor adheres to an approved code of conduct and is registered with the ICO. The admin staff check the processors website with regard to their storage of data.

The school has a duty to report certain types of personal data breaches to the ICO and, in some cases, to the individuals affected.

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

The school will notify the ICO of a breach if it is likely to result in a risk to the rights and freedoms of individuals. A notifiable breach has to be reported to the ICO within 72 hours of the business becoming aware of it.

If this is the case anyone concerned will be notified those concerned directly immediately

In all cases you all records of personal data breaches must be maintained, whether or not they were notifiable to the ICO.

Staff understand what constitutes a personal data breach, and that this is more than a loss of personal data.

The school has an internal breach reporting procedure in place.

Data transfers are made to the following:

CPOMS – system to monitor Child Protection and Safeguarding. Linked to Sims, data is transferred from Sims to CPOMS via a secure cloud network.

O Track – external assessment provider linked to Sims, data is transferred from Sims to O Track. All teachers have a password provided by O Track.

ParentPay – external payment system in school. ParentPay automatically links with the school MIS to update changes to pupil data.

'Data centre security. Our school online payment system is hosted, managed and maintained in a secure and reliable data centre, fully compliant with and certified to ISO/IEC 27001 and PCI DSS.'

School grid/Dolce – a computerised ordering and payment system for pupil meals.

Live Kitchen use industry standard 256 bit encryption protocols to encrypt the communication between an authenticated user's web browser and Live Kitchens' website.'

Evidence Me – a computerised system for observing Early Years.

“access to Evidence me through a modern browser is secured through the latest HTTPS protocols, transports, key exchange and cyphers, TLS 1.2, ECDHE RSA with P-256 and the AES 128 GCM cypher. For customers using older browsers, the site will fallback to older protocols. Therefore, it is the customer's responsibility to use the latest version of a modern browser to ensure maximum security.”

Fischer Family Trust – used for pupil data analysis

*“Our information security processes are externally audited and FFT has certifications for **ISO27001** (the international standard for information security) and **Cyber Essentials Plus** (the UK government standard for information security). We store, process and manage all data in the UK at Amazon Web Services' data centre in London.”*

Secure Access - the S2S system allows schools and local authorities to securely share pupil information, teacher information and upload the school census. Access to S2S is only available via secure access, a secure point of entry for data transfer services.

'Secure as the transfer of information is encrypted (in a code) whilst access to the assessments are secured by complex passwords.'

EntrySign – a signing in system for Staff, pupils and visitors. Pupil data is transferred from Sims to EntrySign for the secure transfer of controlled data.

Data Disposal

The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

Disposal of IT assets holding data shall be in compliance with ICO guidance:

https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf

The school will comply with the disposal of pupil's academic information in compliance with the guidance in IMRS Information and Records Management Toolkit for Schools:

<http://irms.org.uk/page/SchoolsToolkit>

St Ann's R C Primary School
Privacy Notice for Pupils - Data Protection Act 1998

St Ann's R C Primary School are the Data Controller for the purposes of the Data Protection Act. We collect information about your child and may receive information from the previous school and the Learning Records Service.

This information includes your child's contact details, national curriculum assessment results, attendance information [1] and personal characteristics such as ethnic group, special educational needs and any relevant medical information.

We hold this personal data and use it to:

- Support your child's teaching and learning;
- Monitor and report on your child's progress;
- Provide appropriate pastoral care, and
- Assess how well your school is doing and the quality of our services
- To comply with the law regarding data sharing

We will not give information about your child to anyone outside the school without your consent unless the law and our rules allow us to.

Requesting access to personal data

All individuals whose data is held by us, has a legal right to request access to such data or information about what is held and should be made in writing to:

Mrs Maria Noctor
St Ann's R C Primary School
Derbyshire Lane
Stretford
M32 8SH

The identity of the person requesting information must be checked prior to releasing information. The School has the right to restrict the release of information should it adversely affect the rights and freedoms of others.

Plan how SARs are responded to with template letters and checklists to follow, providing a standardised response.

Although the fee has been removed for SAR requests, a School can still charge for excessive and repetitive requests.

Response to SARs must be in a timely manner and within 30 days, but this can be extended to up to an extra 2 months where requests are complex or numerous; but this must be stated to the person making the SAR.

Retention Policies must state how long information is kept by the School and can be referred to if stating that requested information is no longer held by the School.

If you require more information about how the Local Authority (LA) and/or DfE store and use your child's information, then please go to the following websites:

www.trafford.gov.uk

<http://www.teachernet.gov.uk/management/ims/datamanagement/privacynotices/pupilsdata/>

<http://www.teachernet.gov.uk/management/ims/datamanagement/privacynotices/pupilsdata/thirdpartyorgs/>

If you are unable to access these websites, please contact the LA or DfE as follows:

Trafford Council
Trafford Town Hall
Talbot Road
Stretford
Manchester. M32 0TH

Public Communications Unit
Department for Education
Sanctuary Buildings
Great Smith Street. London. SW1P 3BT
Website: www.education.gov.uk
email: info@education.gsi.gov.uk
Telephone: 0870 000 2288

St Ann's R C Primary School

Privacy notice for Staff - Data Protection Act 1998

St Ann's R C Primary School are the Data Controller for the purposes of the Data Protection Act. Personal data is held by the school / Local Authority (LA) about those employed or otherwise engaged to work at the school or LA. This is to assist in the smooth running of the school and/or enable individuals to be paid. This personal data includes some or all of the following: identifiers such as name and National Insurance Number; characteristics such as ethnic group; employment contract and remuneration details; post "A" level qualifications; and absence information.

We hold this school workforce data to and use it to:

- Enable the development of a comprehensive picture of the workforce and how it is deployed
- Allowing better financial modelling and planning
- Inform the development of recruitment and retention policies
- Enable individuals to be paid
- Supporting the work of the School Teacher Review Board and the School Support Staff Negotiating Body

We are required to pass on some of this data to:

The LA
The Department for Education

If you require more information about how the LA and/or Department for Education store and use this data please see our 'how school data is used' page or visit the Department for Education website.

Collecting staff information

Whilst the majority of staff 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 staff information to us or if you have a choice in this.

Storing staff data

We hold staff data while they are on roll.

Their network account is deleted when the member of staff leaves the school.

Any other data required for legal purpose will remain on file and archived.

Who do we share staff information with?

We sometimes need to share the personal information we process with the individual themselves and also with other organisations. Where this is necessary we are required to comply with all aspects of the Data Protection Act (DPA).

Where necessary or required we share information with:

- Trafford Borough Council
- The Department for Education (DfE) and central government
- Education, training, careers and examining bodies
- School staff and boards

- Family, associates and representatives of the person whose personal data we are processing
- Financial organisations
- NHS and healthcare professionals
- Social and welfare organisations
- Law enforcement organisation and courts
- Current, past or prospective employers
- Business associates and other professional advisers
- Suppliers and service providers
- Financial organisations
- Security organisations
- School trips organisations

Data collection requirements

The DfE collects and processes personal data relating to employees. To find out more about the data collection requirements placed on school by the DfE including the data that we share with them, go to the following website: <http://www.gov.uk/education/data-collection-and-censuses-for-schools>

For more information about the department's data sharing process, please go to the following website:

<http://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

Requesting access to personal data

All individuals whose data is held by us, has a legal right to request access to such data or information about what is held and should be made in writing to:

Mrs Maria Noctor
 St Ann's R C Primary School
 Derbyshire Lane
 Stretford
 M32 8SH

Staff 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 ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/>