St Luke's RC Primary School

GDPR Policy
August 2018

"At St. Luke's School we follow the example of Christ. By being God's disciples here on Earth. We strive to be the best that we can be. To do the best that we can do and to make God proud."

Policy Number	1
Target Audience	All stakeholders
Approving Committee	FGB
Last Review Date	August 2018
Next Review Date	-
Policy Author	Andrew Van Dams

Version Control			
Version No	**Date Approved**	**Reviewed By**	**Changes**
V1.0 Data Protection policy template for schools	31/08/18	Andrew van Damms	

1. Introduction

The processing of personal data is essential to the delivery of core education activities in schools. *St Luke's RC Primary School* recognises that compliance with Data Protection legislation (principally the General Data Protection Regulation (GDPR) and Data Protection Act 2018) will ensure that such processing is carried out fairly, lawfully, and transparently.

Data protection legislation, and Article 8 of the European Convention on Human Rights recognise that there is a balance between the legitimate use of personal data by organisations to enable the effective and efficient delivery of services in the public interest and ensuring appropriate protection for the rights and freedoms of the individual(s) to whom the personal data relates.

The school welcomes the increased protection that GDPR provides in relation to personal information about children. Indeed the school recognises the very considerable responsibilities it has to safeguard the personal information it holds about its pupils and this comprehensive policy sets out how the school will go about ensuring it meets its obligations.

2. Scope

This policy applies to the collection, use, sharing and other processing of all personal data held by the School, in any format including paper, electronic, audio and visual. It applies to all employees, whether employed on a permanent, fixed term, or temporary (agency) basis.

3. 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 category personal data	Personal data which is more sensitive in nature and which requires 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.

4. Personal data processed by the school

The school processes personal data relating to parents, pupils, staff, governors, visitors and others in order to be able to carry out its core education functions. Examples include:

- A name and address or contact details held about pupils, parents and staff and their families
- Information attached to a reference number that could be used to identify someone
- A pupil's school record
- Photographs of a child
- Records of sickness absence
- Financial records relating to a child's parent.

The school determines the purposes and means of processing this personal data and so is a data controller. The school is registered as a data controller with the ICO and will renew this registration annually as required.

The School will produce and maintain a record of its processing activities ('ROPA') and make this available to the Office of the Information Commissioner ('ICO') upon request. Appropriate information concerning the processing of personal data (e.g. why, how, for how long) in respect of which the school is a data controller will be communicated by the school to data subjects by means of appropriate privacy notices.

5. Roles and responsibilities

Data protection officer

The Data Protection Officer (DPO) is provided through the GDPR SLA service which the school purchases via Salford City Council. The DPO is responsible for overseeing the implementation of this policy, monitoring the school's compliance with Data Protection law, and developing related policies and guidelines where applicable.

The DPO's contact details are below:

Andrew Van Damms
Legal & Governance Division
Service Reform
Salford City Council
Civic Centre
Chorley Road
Swinton
M27 5AW

Email: andrew.vandamms@salford.gov.uk
Tel: 0161 793 3957

Headteacher

The Headteacher acts as the representative of the data controller 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 school of any changes to their personal data, such as a change of address
- Contacting the DPO/seeking advice via the council's SLA service in the following circumstances:
  - o With any questions the school is not immediately able to resolve about the operation of this policy and about GDPR/DPA 2018, for example in relation to the lawful use, secure handling, and retention of personal data,
  - o Where Data Protection rights have been exercised, e.g. subject access, right to erasure etc, and it is unclear what the school needs to do to meet its obligations
  - o If there has been a data breach
  - o When engaging in a new activity that may affect the privacy rights of individuals and assistance is required to conduct a Data Protection Impact Assessment (DPIA).
  - o If assistance is required in order to ensure Data Protection requirements are met when carrying out procurement and contracting activity e.g. where another organisation may need to process personal data on behalf of the school.

6. Data Protection Principles

The School will comply with the principles relating to the processing of personal data set out in the GDPR by putting in place processes to ensure that personal data is:

- processed lawfully, fairly and in a transparent manner in relation to the data subject

(**'lawfulness, fairness and transparency'**);

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**'purpose limitation'**);
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**'data minimisation'**);
- accurate and, where necessary, kept up to date (**'accuracy'**);
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (**'storage limitation'**);
- 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 (**'integrity and confidentiality'**).

The School shall be responsible for, and be able to demonstrate compliance with, the above principles (**'accountability'**).

7. Collecting Personal Data

a. Lawfulness, fairness and transparency

The school will only process personal data where it has met one of 6 'lawful bases' (legal reasons) to do so under Data Protection law:

- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- 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 for the **legitimate interests** of the school 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 pupil) has freely given clear **consent**

For special categories of personal data, the school also needs to meet one of the special category conditions for processing as set out in Article 9 of the GDPR (as supplemented by the DPA 2018). The conditions which the school will mainly rely on are:

- Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law
- Processing is necessary for carrying out obligations under employment, social security or social protection law
- Processing is necessary to protect the vital interests of a data subject or another individual

- Explicit consent of the data subject

The school is keenly aware of the additional protections set out in GDPR for personal data about children and takes its responsibilities very seriously. If the school offers online services to pupils, such as classroom apps, particular regard will be had for GDPR requirements in relation to the provision of Information Society Services to Children. In particular, the school will ensure it obtains parental consent (except for online counselling and preventive services) in line with relevant requirements based on the age of the child.

Privacy Notices

When collecting personal data from pupils, parents/carers, employees, and governors the school will ensure that relevant information is provided setting out why/how the council will be using the information, how long it will be kept for, and how individual rights can be exercised. The school has produced three separate privacy notices, one for pupils/parents, one for staff, and one for governors.

b. Limitation, minimisation, accuracy and retention

Personal data will only be collected for specified, explicit and legitimate reasons and only to the extent that is necessary to carry out our education functions. If personal data is to be used for reasons other than those given when it was first obtained, the school will generally inform the individuals (or parents/carers) concerned before doing so and seek consent if it is necessary to do so. An exception to this may be where it is necessary and imperative to share information where there are safeguarding concerns or in the event of an emergency.

The school will ensure there are robust measures in place to ensure that the personal data it holds is accurate and kept up to date. This will include proactive actions in the form of regular quality checks of records, and appropriate remedial actions to amend/update records In any case where the school becomes aware of any inaccuracy in the personal data it holds.

The school will retain personal data only for as long as is necessary in accordance with statutory and operational requirements. The school has a comprehensive records management policy and retention schedule which sets out the length of time specific types of record need to be retained for and the actions the school will take to ensure secure destruction/disposal.

8. Sharing Personal Data

There are situations where the school may legitimately need to share information, for example:

- there is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- additional help and support is available from other agencies – consent from parents/carers will be needed where the nature of support or interventions are of the type which would require their agreement

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

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes

The school may also share personal data with emergency services and the local authority to help them to respond to an emergency situation that affects any of our pupils or staff.

Data processors

Suppliers/contractors may need to be provided with personal data in order to provide services to the school or deliver services on behalf of the school e.g. IT companies providing software platforms to the school. When doing this, the school will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law, in particular in relation to information security
- Ensure a data processor agreement is put in place between the school and the contractor/supplier

9. Subject Access Requests and other Rights of

Individuals a. Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal data that the school holds about them. This includes:

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

Subject access requests will usually be made in writing (e.g. by letter or email) but can also be made verbally. A request should include:

- Name of individual
- Correspondence address
- Details of the information requested

b. Children and subject access requests

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

.

Children below the age of 12 (Primary School):

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, in many cases parents/carers will be able to exercise subject access rights access requests on behalf of pupils. This is not an absolute rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above (Secondary School):

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, subject access requests from parents or carers of pupils will only be granted with the express permission of the pupil. This is not an absolute rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

c. Responding to subject access requests

When responding to requests, the school:

- Will ask the individual to provide two forms of identification unless the school is otherwise satisfied of the identity of the person making the request
- Will respond without delay and within one month of receipt of the request
- Will provide the information free of charge
- May extend the timescale for compliance by a further two months, where a
- request is complex or involves very large volumes of information. Where this is the case, the school will inform the individual of this within one month, and explain why the extension is necessary

The school will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil 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, the school 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 the school refuses a request, it will will tell the individual why, and tell them they have the right to complain to the ICO.

d. Other Data Protection rights of the individual

Individuals have a number of additional rights, including:

- the right to rectification i.e. to have inaccurate personal data rectified
- the right to erasure i.e. to have personal data erased – this is not an absolute right and only applies in certain circumstances
- the right to restriction – this means personal data can still be stored but not used. This is not an absolute right and only applies in certain circumstances
- the right to object to processing – a data controller can continue to process personal data if it can demonstrate it has compelling reasons to do so. Individuals have an absolute right to stop their personal data being used for direct marketing
- rights in relation to automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)

These rights can be exercised in writing or verbally. In most cases, the school has one calendar month in which to respond. The DPO/council will be contacted for advice via the SLA service in the event the school is unsure how to handle any such request.

10. Parental right of access to Education records

The Education (Pupil Information) (England) Regulations 2005 allow parents access to the official education records of their children. The school must make a pupil's educational record available for inspection or provide a copy of the record within 15 school days of a valid written request by a parent. Any charges for copying will not exceed the cost of supply.

The school may refuse to disclose information under the Pupil Information Regulations where:

- The school would have no right to disclose the information to the pupil under the GDPR and DPA 2018.
- This may be where the information might cause serious harm to the physical or mental health of the pupil or another individual.

Steps need to be taken to verify the identity of the person making the request as is the case when handling subject access requests.

11. Biometric Recognition Systems

If and where the School uses pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash), the school will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before taking any biometric data from their child and processing it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). If a biometric system is introduced, alternative means of accessing the relevant services will be provided for those who do not wish to participate. For example, pupils can pay for school dinners in cash at each transaction if they wish.

Parents/carers and pupils can withdraw their consent from participation in a school's biometric recognition system(s) at any time. In such cases the school will ensure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, the school will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), the school will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they do not wish to use it. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

12. CCTV

The School uses CCTV in various locations around the school site for the purposes of crime prevention, maintaining site security and for public safety. In doing so, the school will follow ICO guidance along with other relevant industry codes of practice in relation to the use of CCTV.

Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

14. Data Protection by Design & Default

The School's approach to compliance with data protection legislation will be underpinned by the principles of privacy by design and privacy by default.

'Privacy by design' means that the school will take into account privacy issues from the very outset of planning for an activity that might involve the processing of personal data. When undertaking a new activity privacy considerations will be embedded throughout.

Data Protection Impact Assessments will be carried out with support from the council's SLA service where required and oversight from the DPO.

'Privacy by default' means that the School will ensure that only personal data that is necessary for a specific purpose is processed. The School will not collect more personal data than is needed for the purposes concerned, process it in any ways other than than is necessary or store it longer than is needed.

15. Data Security & Storage of Records

The school has appropriate physical, technical and organisational measures in place in order to ensure the security of personal data.

In particular:

- Ensuring authorised access (i.e. that only people who have a need to know the personal data are authorised to access it);
- 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
- Where personal information needs to be taken off site, this is kept to the minimum required and staff must sign it in and out from the school office
- Strong Passwords that are at least 8 characters long containing a mixture of letters, numbers and special characters required to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices where personal information is stored
- Where the school engages a data processor, due diligence is carried out to ensure stored securely and adequately protected

16. Disposal of Records

This is covered in the school's records management policy.

17. Personal Data Breaches

The school has robust measures in place to protect the personal data it holds. However, in order to be prepared for any possible incident a data breach management policy has been produced. All staff will be briefed on this. It is essential all staff understand that appropriate and necessary actions need to be taken quickly in order to remedy a breach and in order to ensure, in the event of a serious incident, the school is in a position to notify the ICO within 72 hours.

18. Training

The school recognises that data protection training is crucial so that all staff understand their responsibilities relating to Data Protection and the use of personal data. Failure to

comply with data protection legislation could lead to serious consequences, and in some cases may result in significant fines or criminal prosecution.

All staff and governors are provided with data protection training as part of their induction process. The school will also ensure attendance at training and awareness sessions to be provided by the council through the SLA service and ensure this learning is cascaded within the school accordingly.

19. Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy. The policy will be reviewed annually and updated if necessary.

The school will ensure that all staff are aware of and have read this policy. This policy will also be shared with the full governing board.

20. Links with Other Policies

This data protection policy is linked to other policies including:

- Records Management and Retention policy
- School records retention schedule
- Data breach management policy