St. Columba's Roman Catholic Primary School

Data Protection Policy

Origin: Information Governance Team – North Tyneside Local Authority

Head Teacher: Mrs. C. Jordan

This Policy was ratified by St. Columba's Governing Body in May 2018

Signed by the Head Teacher: *Mrs C. Jordan*

Signed by the Chair of Governors: *Mr. P. Dinsley*

Date of next review:

This policy will be reviewed in May 2020 or sooner if deemed necessary. All staff and governors will be consulted as to its effectiveness as part of the review process.

Requests for copies - If a signed paper copy of this policy is requested, the school office will provide this free of charge.

1. Introduction and purpose

1.1. St. Columba's Catholic Primary School (**School**) is committed to ensuring that all personal data about staff, pupils, parents, governors, volunteers, visitors and all other individuals is collected, stored and processed in accordance with the law and relevant guidance from the Information Commissioner's Office (**ICO**), in particular the:

1.1.1. General Data Protection Regulation (**GDPR**);

1.1.2. expected provisions of the Data Protection Act 2018 (**DPA**);

1.1.3. Regulation 5 of the Education (Pupil Information) (England) Regulations 2005; and

1.1.4. ICO's Code of Practice for the use of surveillance cameras and personal information.

1.2. St. Columba's Catholic Primary School is registered with the ICO as a Data Controller for the processing of living individuals' personal information. The School Data Protection Policy has been produced to ensure its compliance with the GDPR. The Policy incorporates guidance from the ICO, and outlines the Schools overall approach to its responsibilities and individuals' rights under the GDPR.

1.3. The GDPR and DPA give individuals rights over their personal data and protect individuals from the erroneous use of their personal data. This Policy outlines the School's overall approach to its responsibilities under the law. It applies to all personal data, regardless of whether it is in paper or electronic format.

1.4. This Policy applies to all employees (including temporary, casual or agency staff and contractors, consultants and suppliers working for, or on behalf of, the School), third parties and others who may process personal information on behalf of the School. The School is the Data Controller for the purposes of the relevant law.

1.5. The Policy also covers any staff and pupils who may be involved in research or other activity that requires them to process or have access to personal data, for instance as part of a research project or as part of professional practice activities. If this occurs, it is the responsibility of the School to ensure the data is processed in accordance with the GDPR and that pupils and staff are advised about their responsibilities.

2. Types of data covered by this Policy

2.1. Personal data is information relating to an individual (**data subject**) who can be identified from that data alone, or in conjunction with other information held. This includes written data (including the expression of opinions about an individual), telephone, audio or video recordings and photographs. The personal data may be held manually or electronically and compiled, stored or otherwise processed by the School, or by a third party on its behalf.

2.2. "Special categories" of personal data relates to personal data which is more sensitive, including information relating to an individual's:

- racial or ethnic origin;
- political opinions, religious beliefs or other beliefs of a similar nature;
- membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
- physical or mental health or condition;
- sexual life or sexual orientation;
- biometric /genetic data; or
- any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

3. The Data Protection Principles

3.1. The law requires the School, its staff and others who process or use any personal information to comply with the Data Protection Principles.

3.2. These principles require that personal data shall:

- be obtained and processed fairly and lawfully, in a transparent manner in relation to individuals and not be processed unless certain conditions are met;
- be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose;
- be adequate, relevant and not excessive for those purposes;
- be accurate and, where necessary, kept up to date;
- 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; and
- 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.

4. Roles and responsibilities

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

Governing Board

4.2. The Governing Board has overall responsibility for ensuring that the School complies with all relevant data protection obligations.

Data Protection Officer

4.3. The School has an appointed Data Protection Officer (**DPO**) to handle day-to-day issues which arise, and to provide members of the School with guidance on Data Protection issues to ensure they are aware of their obligations.

4.4. The 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.

4.5. They will provide an annual report of their activities to the Governing Board and, where relevant, report to the Board their advice and recommendations on school data protection issues.

4.6. The DPO is also the first point of contact for individuals whose data the school processes, and for the Information Commissioner's Office (**ICO**).

4.7. Our DPO is:

Data Protection Officer (for Schools)
Law and Governance
North Tyneside Council
Quadrant
The Silverlink North
Cobalt Business Park
North Tyneside
NE27 0BY

Telephone: (0191) 643 2333

Fax: (0191) 643 2431

Email: dpo.schools@northtyneside.gov.uk

Headteacher

4.8. The Headteacher acts as the representative of the Data Controller on a day-to-day basis.

All staff

4.9. All members of staff must:

- familiarise themselves and comply with the data protection principles;
- ensure any possession of personal data is accurate and up to date;
- ensure their own personal information is accurate and up to date;
- keep personal data for no longer than is necessary in line with retention guidelines;
- ensure that any personal data they process is secure and in compliance with the School's information-related policies and strategies;
- ensure personal data is only used for those specified purposes and is not unlawfully used for any other business that does not concern the School;
- obtain consent (where required) for collecting, sharing or disclosing personal data;
- acknowledge data subjects' rights (e.g. right of access to all their personal data held by School) under GDPR, and comply with access to those records;
- contact the DPO where any request is received for access to personal data or where they have any concerns or doubt relating to data protection to avoid any infringements of the relevant law.

Pupils

Pupils, of St. Columba's Catholic Primary School are expected to:

- Comply with the data protection principles
- Comply with any security procedures implemented by St. Columba's Catholic Primary School.

Training

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

5. How the School processes personal data

5.1. The School will only process personal data where it has 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 **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 so that the school 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 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 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**

5.2. For "special categories" of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and DPA.

5.3. If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

5.4. Upon acceptance of employment at the School, members of staff consent to the processing and storage of their data in accordance with the data protection principles.

5.5. 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. Individuals are also informed about how their data will be processed via the relevant Privacy Notices, which are published on our website or available from the School Office (as appropriate).

5.6. 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 where necessary.

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

6. Retention, Security and Disposal

6.1. The personal data the School holds will only be retained for as long as is necessary to comply with our legal obligations and complete the task for which we hold the data.

6.2. Recipients responsible for the processing and management of personal data need to ensure that the data is accurate and up-to-date. If an employee, student or applicant is dissatisfied with the accuracy of their personal data, then they must inform the School.

6.3. Personal information held in paper and electronic format shall not be retained for longer than is necessary. In accordance with Article 5 of the General Data Protection Regulations, personal information shall be collected and retained only for business, regulatory or legal purposes.

6.4. In accordance with the provisions of the GDPR, all staff whose work involves processing personal data, whether in electronic or paper format, must take personal responsibility for its secure storage and ensure appropriate measures are in place to prevent accidental loss or destruction of, or damage to, personal data.

6.5. Any staff working from home or away from the School premises will be responsible for ensuring that personal data removed from School premises is stored securely and is not accessible to others. Personal data should only be removed from School premises for as long as is necessary to complete the particular task.

6.6. When staff no longer need the personal data they hold, they must ensure it is dealt with in accordance with the Retention Schedule. Personal data in paper format must be shredded or placed in the confidential waste bins provided. Personal data in electronic format should be deleted, and CDs and pen drives that hold personal data passed to our I.T provider for safe disposal. Hardware should be appropriately degaussed in compliance with our I.T service provider contract and in line with DPA and GDPR requirements.

7. Obtaining, Disclosing and Sharing Personal Data

7.1. Only personal data that is necessary for a specific School related business reason should be obtained.

7.2. Pupils and their parents and or Carers will be informed about how their data will be processed.

7.3. Upon acceptance of employment at St. Columba's Catholic Primary School, members of staff also consent to the processing and storage of their data.

7.4. Data must be collected and stored in a secure manner.

7.5. Personal information must not be disclosed to any third party organisation without prior consent of the individual concerned. This also includes information that would confirm whether or not an individual is or has been an applicant, pupil or employee of St. Columba's Catholic Primary School.

7.6. The School may have a duty to disclose personal information in order to comply with legal or statutory obligations. GDPR allows the disclosure of personal data to authorised bodies, such as the police and other organisations that have a crime prevention or law enforcement function.

7.7. Personal information that is shared with third parties on a more regular basis shall be carried out under written agreement to stipulate the purpose and boundaries of sharing. For circumstances where personal information would need to be shared in the case of ad hoc arrangements, sharing shall be undertaken in compliance with the GDPR 2018.

7.8. The School will not normally share personal data with anyone else without the consent of a data subject (including information that would confirm whether or not an individual is or has been an applicant, student or employee of the School), but in some circumstances it may have a duty to disclose personal information in order to comply with a legal or statutory

obligation. Our Privacy Notices contain more detail about circumstances where we may need to share data.

7.9. Examples of circumstance where we may share personal data include, but are not limited to where:

- there is an issue with a pupil 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
- our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
  - only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law;
  - 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; and
  - only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

7.10. 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
- 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, as long as personal data is sufficiently anonymised or consent has been provided

7.11. 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 pupils or staff.

8. Transferring Personal Data

8.1. Any transfer of personal data will be done securely.

8.2. Where any personal data must be transferred by email the School will only do so where the data can be encrypted with a password provided to the recipient by separate means such as via telephone.

8.3. All staff must take care to ensure emails containing personal data are not send to unintended recipients. It is important that emails are addressed correctly and care is taken when using reply all or forwarding or copying others in to emails. Use of the blind copy facility should be considered when sending an email to multiple recipients to avoid disclosing personal information to others.

8.4. Personal email accounts should not be used to send or receive personal data for a work purpose.

8.5. Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Right of access the information held (Subject Access Requests)

9.1. Individuals have the right of access to their personal data held by the School. This applies to data held in both paper and electronic format, and within a relevant filing system.

9.2. The School shall use its discretion under the DPA to encourage informal access at a local level to a data subject's personal information, but it will also have a formal procedure for the processing of Subject Access Requests.

9.3. Any individual who wishes to exercise this right should make the request in writing; either by letter, email or fax to the DPO (see details above). The request should include:

- Name of individual whose data is requested (and the person making the request, if a third party)
- Correspondence address
- Contact number and email address
- Details of the information requested

9.4. If staff receive a Subject Access Request they must immediately forward it to the DPO.

10. 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.

11. 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, most Subject Access Requests from parents or carers of pupils at our School may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

12. Responding to subject access requests

12.1. When responding to requests, we:

- may ask the individual to provide 2 forms of identification;
- may contact the individual via phone to confirm the request was made;
- will respond without delay and within 1 month of receipt of the request;
- will provide the information free of charge; or
- 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.

12.2. We 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; or
- is given to a court in proceedings concerning the child.

12.3. 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.

12.4. If we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

13. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

14. Photographs and videos

14.1. As part of our school activities, we may take photographs and record images of individuals within our school.

14.2. We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

14.3. Uses may include:

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

14.4. Consent can be refused or withdrawn at any time but requests must in writing to the School Office if this is during the school year. Consent will be obtained at the start of every academic year. If consent is withdrawn, we will remove the photograph or video and not distribute it further.

15. Data Security Breaches

15.1. The School will take all reasonable precautions to ensure that there are no personal data breaches. We recognise it is important to respond to any potential breach quickly and effectively. A breach may arise from a theft, a deliberate attack on School systems, and unauthorised use of personal data, accidental loss or equipment failure. In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

15.2. Each incident will be investigated and judged on its individual circumstances and addressed accordingly. If appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium;
- Safeguarding information being made available to an unauthorised person;
- A deliberate attack on school or third party IT provider's systems; or
- The theft of a school laptop or other portable device containing non-encrypted personal data about pupils.

16. Links with other policies

16.1. This Policy is linked to our:

- Records Management Policy;
- Privacy Notices;
- Acceptable Use Policy
- Information Security Procedures
- Safeguarding and Child Protection Policy – [***to keep this list under review***]

17. Monitoring arrangements

17.1. This Policy has been approved by and has the full ownership of the Governing Board. It will be reviewed and updated (if necessary) at least every 2 years and shared with the Governing Board.

APPENDIX 1

DATA BREACH REPORT FORM

Please act promptly to report any data breaches. If you discover a data breach, please notify the Head Teacher of it immediately and complete Section 1 of this report.

The Head Teacher (or School Office on the Head's behalf) will inform our DPO and investigate the next steps required. DPO email address: dpo.schools@northtyneside.gov.uk

Section 1: Notification of Data Security Breach	**To be completed by individual reporting incident**
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	
For use by the Data Protection Officer	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity	**To be completed by the Lead Investigation Officer in consultation with the Head Teacher if appropriate IT where applicable**
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the School/Academy or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK personal data • Special Category data (as defined in the Data Protection Act) relating to a living, identifiable individual's a) Racial or ethnic origin; b) Political opinions or religious or philosophical beliefs; c) Membership of a trade union; d) Physical or mental health or condition or sexual life; e) Biometric data	
• Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas;	
• Personal information relating to parents, staff and children	
• Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
• Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals	
• Security information that would compromise the safety of individuals if disclosed.	

Section 3: Action taken	To be completed by Data Protection Officer and/or Lead Investigation Officer
Incident number	**e.g. year/001**
Report received by:	
On (date):	
Action taken by responsible officer/s:	
Was incident reported to Police?	**Yes/No** **If YES, notified on (date):**
Follow up action required/recommended:	
Reported to Data Protection Officer and Lead Officer on (date):	
Reported to other internal stakeholders (details, dates):	
For use of Data Protection Officer and/or Lead Officer:	
Notification to ICO	**YES/NO If YES, notified on:** **Details:**
Notification to data subjects	**YES/NO If YES, notified on:** **Details:**
Notification to other external, regulator/stakeholder	**YES/NO If YES, notified on:** **Details:**