Blackburn with Darwen Borough Council

Schools Data Protection Policy

(GDPR)

Vision:

In our family school, we strive to be the best for today, for tomorrow, for ourselves, for each other, the wider world and for God.

As a Christian family we nurture an understanding that we are all of equal value and infinite worth.

In the safety of our unique family we will flourish and grow towards being Global Citizens and Courageous Advocates.

('You are now citizens together with God's people and members of the family of God'. Ephesians 2:19)

Mission statement:

Learning to love, loving to learn in the family of Christ.

('Encourage one another and build each other up'- 1 Thessalonians 5:11)

Contents

1.	Introduction	3
2.	Definitions	3
3.	Data Protection Principles	4
4.	Lawful Processing	4
5.	Consent	5
6.	Accountability and Governance	5
6.1.	Data Protection Officer (DPO)	5
6.2.	Register of Processing Activities (RoPA)	6
6.3.	Workforce Training	6
6.4.	Data Protection Impact Assessments (DPIA's)	6
6.5.	Contracts	6
7.	Individual Rights	6
7.1.	Right to be informed	6
7.2.	Right of Access	7
7.3.	Individual rights	7
8.	Data Security	7
9.	Breach Reporting	8
10.	Data Retention	8
11.	Data Accuracy and Limitation	8
12.	Information Requests	9
13.	CCTV (delete if not applicable) and Biometric Data	**Error! Bookmark not defined.**
14.	Appendices	10
Appendix A - Breach Reporting Procedure		10
Appendix B - Privacy Notice (How we use school workforce information)		11

1. Introduction

St Cuthbert's CE Primary School collects, holds and processes personal data about pupils, staff, parents/carers, governors, visitors and other individuals who have contact with the school. It therefore has a number of legal obligations under the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

Within this policy we will set out how we seek to protect personal data and ensure that employees understand the rules governing their use of personal data to which they have access in the course of their employment. This policy applies to all personal data, regardless of whether it is held in paper or electronic format.

The school is a registered data controller with the Information Commissioner and will continue to abide by the new registration arrangements. All members of staff have responsibility for how the school collects, holds and processes personal data. The policy therefore applies to all staff as well as external organisations or individuals processing data on behalf of the school. Staff who do not comply with this policy may face disciplinary action.

This policy also commits that the school will also comply with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, the Protection of Freedoms Act 2012 when referring to use of biometric data and Article 8 of the Human Rights Act 1998.

2. Definitions

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR refers to sensitive personal data as 'special categories of personal data'. Special category data is personal data which the GDPR says is more sensitive, and so needs more protection. For example, information about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life or sexual orientation, are all 'special categories of personal data'.

The GDPR applies to 'controllers' and 'processors'. The school is a data controller who determines the purposes and means of processing personal data. A processor is responsible for processing personal data on behalf of a controller.

3. Data Protection Principles

Under Article 5 of the GDPR, the data protection principles set out the main responsibilities for organisations. It states personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f) 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."

Article 5(2) requires that:
"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

4. Lawful Processing

The first principle requires that organisations process personal data in a lawful manner. The school will only process personal data if it can meet one of the following lawful bases set out under Article 6:
(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
(d) Vital interests: the processing is necessary to protect someone's life.
(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

In addition if the school wishes to process 'special category data', it will identify an additional condition for processing as set out under Article 9.

5. Consent

Where a need exists to request and receive consent of an individual prior to the collection, use or disclosure of personal data, the school is committed to seeking such consent. In all cases consent must be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's wishes. The school is therefore committed to obtaining consent in the following manner:

- consent is presented in a manner clearly distinguishable from other matters
- the request is made in an intelligible and easily accessible form using plain language
- is freely given (i.e. not based on the need to conduct another processing activity)
- the date, method, validity and content of the consent is documented
- a simple method is provided for the data subject to be able to withdraw consent at any time

Once consent is withdrawn by the data subject, the school will cease processing data for the specified purpose without undue delay.

If the school wishes to offer information Society Services (ISS) to pupils it will gain parental consent for any pupil below the age of 13.

6. Accountability and Governance

6.1 Data Protection Officer (DPO)

Under the GDPR it is mandatory for Local Authorities (as defined by the FOIA) to designate a Data Protection Officer (DPO). The DPO's minimum tasks are defined in Article 39:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities

The contact details for the School's designated DPO are as follows:
Lee Gardiner, Data Protection Officer
Blackburn Town Hall (G Floor), Blackburn, BB1 7DY or
Schools.IG@blackburn.gov.uk
Staff should contact the DPO if they have any queries about this policy, data protection law, data retention or the security of personal data. The DPO can also be contacted directly if members of staff have any concerns that this policy is not being adhered to.

6.2 Register of Processing Activities (RoPA)

The school is required to maintain records of activities related to higher risk processing of personal data. The school can confirm it maintains a Register of Processing Activities and this is held by the school office in conjunction with the DPO. All members of staff are required to notify the relevant persons before they embark on any new processing activities so they can be adequately recorded on the RoPA.

6.3 Workforce Training

The school is committed to providing data protection training to all staff as part of their induction process and will issue regular refresh training throughout the course of their employment or in the event of any changes in data protection law. The school will retain a record of this training programme and this will be made available to the supervisory authority on request.
Staff for the purpose of this policy includes **all** staff including student teachers on training placements and these staff would be required to comply with all school policies relating to their appropriate use of personal information.

6.4 Data Protection Impact Assessments (DPIA's)

Data protection impact assessments (DPIAs) are a tool which can help the school identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.
The school will complete DPIA for certain listed types of processing, or any other processing that is likely to result in a high risk to individuals' interests. Therefore staff must consult their DPO before they embark on any new processing that could be regarded as being high risk to individuals' interests. If required the DPO will assist members of staff completing the school's DPIA template.

6.5 Contracts

Whenever a controller uses a processor, it needs to have a written contract in place. This is important so that both parties understand their responsibilities and liabilities. The school contracts include the following compulsory details in its contracts:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subject; and
- the obligations and rights of the controller.

7 <u>Individual Rights</u>

7.1 Right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. We call this 'privacy information' and the school will issue privacy notices in relation to pupil data, workforce data and governor data. The school will endeavour to issue these notices on induction and also make them available on the school's website throughout the data subject's school life. Please note a copy of the workforce privacy notice is contained within Appendix B of this policy.

7.2 Right of Access

Individuals have the right to access their personal data (commonly known as subject access) and supplementary information about the processing of their data. The right of access allows individuals to be aware of and verify the lawfulness of the processing of their personal data. The information that can be requested 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
- 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 can be submitted to the DPO in writing and must contain the name of the data subject, a correspondence address and a description of the information requested. The school will provide the information without delay and at the latest within one month of receipt of the request. The school will not apply a fee to requests unless the request is manifestly unfounded or excessive. The school will take reasonable steps to verify the identification of the applicant and if the applicant wishes to request a review of the school's decision, the process for doing so will be clearly outlined in the response issued.

7.3 Individual rights

GDPR also empowers individuals with the right to rectification, erasure, right to restrict processing, data portability, right to object and rights in relation to automated decision making or profiling. The school will carefully consider any requests under these rights and requests can be made in writing to the school's DPO using the contact details provided above.

8 Data Security

Principle f) states data should be processed in a manner that ensures appropriate security of the personal data. This means the school must have appropriate security to prevent the personal data it holds being accidentally or deliberately compromised. Particular attention will be paid to the need for security of sensitive personal data.

Manual data will be stored where it is not accessible to anyone who does not have a legitimate reason to view or process that data. Staff should carefully consider whether they need to take any manual data offsite before doing so and record instances where any 'special categories of data' is taken offsite. The following measures must be taken by staff in relation to electronic data:

- portable electronic devices, such as laptops, ipads and hard drives that contain personal data are stored in a locked cupboard or draw
- encryption software is used to protect all portable devices and removable media that contain personal data, such as laptops and USB devices
- passwords must meet appropriate security standards, be changed at regular intervals and must not be divulged to any other persons
- where personal data is shared with a third party, staff should carry out due diligence and ensure the data is sent in a secure manner or appropriate measures are taken to mitigate the risk of individuals being identified

- when sending personal data to a third party, staff must carefully check the recipient and their contact details
- where personal devices are used to access organisational email accounts, staff should ensure appropriate passwords are applied to the device and they access the accounts by the recommended means i.e. Office 365 users should use the Office 365 application rather than syncing to phone
- staff should not open links when emails are received from unknown recipients, or the emails appear suspicious
- personal data must be stored in a secure and safe manner, with careful consideration made to who can access the data

9 Breach Reporting

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. Where feasible, the school must do this within 72 hours of becoming aware of the breach, it is therefore essential that **all members of staff make the relevant persons aware of any potential breaches of data protection without undue delay.** This includes all losses, thefts or inadvertent disclosures of personal data. It also includes the loss or theft of any device that holds personal data. The relevant persons will then follow the breach procedure outlined in Appendix A in conjunction with the DPO.
The DPO will investigate all reported incidents to confirm whether a personal data breach has occurred. If a personal data breach is confirmed, the DPO will follow the relevant procedure based on the criticality and quantity of the personal data involved. For significant personal data breaches, the school will carefully consider whether it is required to notify the Information Commissioner and the data subjects affected.

10 Data Retention

Principle f) states data must be 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. Data will only be retained for the specified period outlined in the records management schedule that the school has adopted and will be destroyed in a secure manner thereafter. A copy of the records management schedule is available on request from the school office or from the DPO.

11 Data Accuracy and Limitation

The school will issue regular reminders to staff and parents to ensure that personal data held is up to date and accurate. Any inaccuracies discovered should be rectified and if the inaccurate information has been disclosed to a third party; the recipients will be informed of the corrected data.
The school will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals in the school's privacy notices. 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. Staff must only process personal data where it is necessary to do so in their jobs.

12 Information Requests

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. The school will adhere with 'subject access' requests as outlined in Section 7.2 of this policy.

Personal data will only be disclosed to third party organisations or individuals for whom consent has been given to receive the data, or organisations that have a legal right to receive the data without consent being given e.g. examination boards.

Requests for personal data by the Police or other bodies with law enforcement powers (e.g. HMRC), will usually only be considered when accompanied by a data protection form such as a 'Lancashire Constabulary DP1'. This form typically contains details of the applicant, the purpose of the request and the section of the legislation the information is being requested under. This will allow the DPO to make an informed decision as to whether the request is proportionate for the purposes requested, against the rights of the data subject

If requests are received from parents/carers for the names of pupils in their class (e.g. for Christmas card or birthday invites), only first names will usually be released, however the school reserves the right to refuse any request in its entirety.

Appendices

Appendix A - Breach Reporting Procedure

In the event of a data breach, including a potential breach, the staff member or data processor must immediately notify the DPO or relevant persons. The reporting member of staff will complete Sections 1-3 of the 'Personal Data Breach Form' before submitting to the DPO. The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully lost, stolen, destroyed, altered or disclosed. The DPO will take the following steps:

- Make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.
- Assess the potential consequences, based on how serious they are, and how likely they are to happen.
- Notify the Head teacher or Chair of Governors if felt appropriate.
- Decide whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material. If it's likely that there will be a risk to people's rights and freedoms, the DPO will advise the Headteacher that they must notify the ICO.
- The DPO will document the decision (either way) in Section 7 of the 'Personal Data Breach Form', in case it is challenged at a later date by the ICO or an individual affected by the breach.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

  If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- Notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- Notify the data subject if the breach is likely to result in a high risk to their rights and freedoms.
- Document each breach, irrespective of whether it is reported to the ICO on the 'Personal Data Breach Register'.
- The DPO and Headteacher will discuss each breach to review what happened and how reoccurrence can be prevented.

Appendix B - Privacy Notice (How we use school workforce information)

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

- personal information (such as name, employee or teacher number, national insurance number)
- special categories of data including characteristics information such as gender, age, ethnic group
- contract information (such as start dates, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)
- medical information (such as occupational health reports and medical conditions)

Why we collect and use this information

We use school workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- enable individuals to be paid
- provide training and development for employees

The lawful basis on which we process this information

We collect and use workforce data under the following conditions contained within Article 6(1) of the General Data Protection Regulations:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
(c) Legal obligation: the processing is necessary for you to comply with the law
(d) Vital interests: the processing is necessary to protect someone's life.
(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Where we process special category data we identify an additional processing condition within Article 9(2) of the GDPR:

Collecting this information

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

Storing this information

We hold workforce data for a specified period which is detailed in the School's Retention Schedule which is contained within the IRMS's Information Management Toolkit for Schools. A copy of the retention schedule is available on request from the School's Data Protection Officer.

Who we share this information with

We routinely share this information with:

- our local authority
- the Department for Education (DfE)

Why we share school workforce information

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

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

Data collection requirements

- The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005
- To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

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

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

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

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

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

To contact the department: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact [include details of school email address]

You also have the right to:

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

If you have a concern about the way we are collecting or using your personal data, we 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/

Contact

If you would like to discuss anything in this privacy notice, please contact:

Mr Lee Gardiner
Data Protection Officer
Information Governance Team, Blackburn Town Hall (4th Floor), Blackburn, BB1 7DY or
Schools.IG@blackburn.gov.uk