# Silverhill Primary School

# Data Protection Policy

| | |
|---|---|
| Document owner | *Jason Coupland – School Business Manager* |
| Document author and enquiry point | *Jason Coupland – School Business Manager* |
| Date of document | May 2018 |
| Version | 3.0 |
| Document classification | Official |
| Document distribution | Published via website |
| Review date of document | April 2019 |

## Version Control

To make sure you are using the current version of this policy please check on SiP or contact Jason Coupland when using printed copies.

| Date Issued | Version | Status | Reason for change |
|---|---|---|---|
| May 2018 | 3.0 | Issued | Updated to comply with GDPR |
| | | | |

## Document Approval

| Job Role | Approvers Name | Date Approved |
|---|---|---|
| *School Business Manager* | Jason Coupland | 21 May 2018 |
| | | |

Please tell us if you need this in large print, on audio tape, computer disc or in Braille by contacting the school office.

## Contents

## 1. Purpose and objectives

This policy forms part of the School's commitment to the safeguarding of personal data processed by its staff. Processing has a very broad definition, and includes activities such as creating, storing, consulting, amending, disclosing and destroying data.

Its objectives are:

- To ensure Officers recognise personal data
- To ensure Officers understand the rights of customers in respect of their personal data and the obligations all staff have with respect to personal data.
- To ensure officers comply with data protection laws

## 2. Introduction

The School processes the personal data of living individuals such as its staff, customers and contractors. This processing is regulated by the General Data Protection Regulation (GDPR) 2016.

It is the duty of the School as a data controller to comply with the data protection principles (see section 4 of this policy) with respect to personal data. This policy describes how the School will discharge its duties in order to ensure continuing compliance with the GDPR in general and the data protection principles and rights of data subjects in particular.

## 3. Legislation, guidance and standards

The School has an obligation to make sure that all information systems and processes meet the terms of all relevant legislation and contractual requirements, including the:

- The General Data Protection Regulation (GDPR) 2016
- The Protection of Freedoms Act 2012
- The Human Rights Act 1998
- Privacy and Electronic Communications Regulations 2000
- E-Privacy Regulation 2018
- Regulation of Investigatory Powers Act 2000
- Indecent display (Control) Act 1981
- Obscene Publications Act 1984
- Copyright, Designs and Patents Act 1988
- Theft Act 1978Common Law Duty of Confidentiality
- Equality Act 2010
- Terrorism Act 2006
- Limitation Act 1980
- The Caldicott Principles
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990

- Freedom of Information Act 2000
- Government Security Classification Scheme

If you are not sure of your responsibilities under any of these laws, contact the school office for further information.

## 4. The principles relating to the processing of personal data

The School shall comply with the principles as stated in Article 5 of the GDPR. All staff must adhere to and comply with these principles at all times when processing any personal data as part of their work. The principles are as follows:

- **Lawful, fair and transparent**

Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

- **Limited for its purpose**

Data can only be collected for a specific purpose.

- **Adequate, relevant and not excessive**

Any data collected must be necessary and not excessive for its purpose.

- **Accurate**

The data we hold must be accurate and kept up to date.

- **Retention**

We cannot store data longer than necessary for the purpose in which it is held.

- **Security**

The data we hold must be kept safe and secure and protected against unauthorised or unlawful processing.

## 5. Special Categories of Data

Special categories of data create more significant risks to a person's fundamental rights and freedoms and as such the GDPR imposing stricter conditions on the processing of such data. Special categories of data include:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics
- health
- sexual orientation

In cases where you will be processing such data there is a higher threshold under the Regulations. There are a separate set of conditions, one of which must be satisfied before any data above is processed. These conditions can be found on the ICO's website.

## 6. Criminal Offence Data

Under the GDPR there are specific rules regarding the processing of personal data relating to criminal convictions and offences. Such data shall be carried out only under the control of official authority or when the processing is authorised by law providing for appropriate safeguards for the rights and freedoms of data subjects. The principles in section 4 of this policy will also apply to this data. Even if you have a condition for processing offence data, you can only keep a comprehensive register of criminal convictions if you are doing so in an official capacity.

## 7. Accountability and transparency

As an employee of Silverhill Primary School you must ensure accountability and transparency in all use of personal data. You must show how we comply with each Principle. You are responsible for keeping a written record of how all the data processing activities you are responsible for comply with each of the Principles. This must be kept up to date and must be approved by the DPO.

To comply with data protection laws and the accountability and transparency Principle of GDPR, we must demonstrate compliance. You are responsible for understanding your particular responsibilities to ensure we meet the following data protection obligations:

- Fully implement all appropriate technical and organisational measures
- Maintain up to date and relevant documentation on all processing activities through the completion of the information inventory.
- Conducting Privacy Impact Assessments where required
- Ensuring data sharing agreements are in place when sharing personal data with third parties.
- Implement measures to ensure privacy by design and default, including:
    - Data minimisation
    - Ensuring data is accurate and up to date
    - Ensuring your service areas corporate privacy notice covers any sharing you do to provide transparency.

## 8. Processing data fairly and lawfully

When processing any personal data you must ensure that there is a sufficient legal basis to do so. This is a requirement under the GDPR, it is your responsibility to

ensure that you check the lawful basis for processing or sharing any personal data you process and make sure this is clearly recorded. If you are unsure as to which lawful basis may apply please contact Derby City Council's Information Governance Team on: data.protection@derby.gov.uk or call: 640763.

You must meet at least one of the six conditions before processing any personal data, the conditions can be found at the ICO's website along with guidance as to when they might apply.

***Deciding which condition to rely on***

When making an assessment of the relevant lawful basis, you must first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. You cannot rely on a lawful basis if you can reasonable achieve the same purpose by some other means.

Our commitment to the first principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

## 9. Consent

Consent should not be a default legal basis, you should only request where consent where you do not have an alternative legal basis such as a legal obligation or public interest reason. Under the GDPR, stricter regulations will affect how we ask for and obtain consent to use an individual's personal data. Under the GDPR consent must be clear, informed and unambiguous and most importantly must be opt-in and provided by way of a clear and affirmative action.

## 10. Sharing information with third parties

You must ensure that there is an Information Sharing or Information Processing Agreement is in place when any sharing personal information with third parties external to the School, there may be rare exceptions to this, such exceptions will be dependent on the relationship with the other party/parties, please seek advice from Derby City Council's Information Governance Team if you think an exception applies. Template agreements can be found on the SiP. You must use the template agreements where one is required.

Asset owners must consult with and agree any new Information Sharing or Information Processing Agreements.
You must ensure that any sharing or processing is referenced in your privacy notice. (see s.11 for more information on privacy notices)

There may also be occasions where information needs to be sent to third parties for the purpose of investigating crime or in relation to taxation, in these cases you must consult with Derby City Council's Information Governance Team and seek their advice before disclosing the information.

## 11. Privacy notices

We must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This should be communicated via a privacy notice. We have an obligation to communicate privacy notice information regardless whether we have collected the data directly from the individual, or we have received the information from another source.

Our privacy notice pages on the SiP explain the process and have the corporate templates all team should use. The content of this section will be updated by the 25th May with up to date templates.

The School should ensure that all privacy notices are available on the website where they can be viewed.

All officers when collecting personal data face to face, or over the phone must inform individuals of their right to review the School's privacy notices online or request a hard copy.

## 12. Accuracy of data

All staff within the School must ensure that ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should take steps to amend the information and seek to inform the data subject. If you receive any requests to rectify information you must promptly refer these to Derby City Council's Information Governance Team on: data.protection@derby.gov.uk or call: 640763.

## 13. Data Security

All staff within the School must ensure that they keep personal data secure and take measures to prevent the accidental loss or destruction of the data. All staff should ensure when processing and storing personal data that they:

- Maintain a record of all processing activities
- Ensure you store data on secure systems
- Ensure you send any personal information by secure email when sending externally
- Ensure information is only accessed by and available to certain people who need to see it

The Information Security Policy details all of the relevant information security obligations. **All Officers must comply with the information security policy.**

## 14. Data breaches

Any breach of this policy or of data protection laws must be reported as soon as practically possible and within 24 hours of becoming aware of the incident. This means as soon as you have become aware of a breach. The School has a legal obligation to investigate and report any serious data breaches to the ICO within 72 hours.

Please contact Derby City Council's Information Governance Team for further advice should a breach occur.

In the event of an information security incident; all Officers must comply with the information security policy, specifically s.12.

## 15. Data Storage

Where personal data is stored you must ensure this is done so securely and adhere to the following:

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly.
- Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used
- Derby City Council's Information Governance Team must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones

- All servers containing sensitive data must be approved and protected by security software
- Have regard to the Information Security Policy

## 16. Data Retention

Personal data should only be retained for as long as is necessary for the purpose in which it was collected. You should review the School's Document retention schedule that can be found on the SiP to ensure that you identify and comply with statutory retention periods. In the absence of a strict statutory retention period Information Asset Owners should review the Local Government Association Guidance. Any adopted practices must be compliant and justifiable with the necessity principle imposed by data protection legislation.

## 17. Transferring data outside of the EEA

The GDPR has strict guidelines regarding the sharing of information outside of the European Economic Area (EEA) and to countries outside of the privacy shield. Please refer to the following guidance on the ICO website that provides further guidance and detail around sharing information outside the EEA and the relevant considerations.

If you are considering transferring data to another country please consult with Derby City Council's Information Governance Team in the first instance and they will advise you on whether the transfer can take place.

## 18. Privacy Impact Assessments

At the start of any project where the processing of personal data will be taking place you need to consider whether a privacy impact assessment will be required. These are mandatory in cases where sensitive data is being processed or where a project involved new technology or some form of surveillance.

In cases where one is required this must be completed at the earliest stage of any project so that the risks are assessed at the outset. Once complete a copy must then be sent to Derby City Council's Information Governance Team on: data.protection@derby.gov.uk so that we can advise

There are a number of screening questions on the PIA template that can be found on the SiP to help you decide if one is required.

## 19. Rights of individuals

Under the GDPR individuals have a number of rights in respect of the personal data we hold about them, the School must ensure that individuals can exercise these rights. All Officers must recognise any of the following rights as statutory rights:

- Right to be informed – through privacy notices
- Right of access – enabling individuals to access their information through a subject access request (see section 20 for more details).
- Right to rectification – amending or rectifying personal data that is inaccurate or incomplete
- Right to erasure – deleting or removing an individual's data on request subject to certain exceptions
- Right to restrict processing – individuals' right to restrict, block or otherwise suppress the processing of their personal data.
- Right to data portability – individuals' right to have their data transferred or provided to them in a machine-readable format
- Right to object – individuals' right to object to their data being processed in certain circumstances
- Rights in relation to automated decision making and profiling

All Officers must promptly refer any of the above statutory request to Derby City Council's Information Governance Team in no more than two working days so that we can advise on the next steps.

Not all data protection rights are absolute; Officers shouldn't agree to or take any action toward complying with any requests without seeking advice from the Council's IG team.

We strongly advise that where possible Officers/requestors use our template form available on the SiP to ensure all the relevant data is captured.

## 20. Subject Access Requests

Individuals have a right to access any personal information the School holds about them subject to certain exemptions. Such a request can be received electronically, letter or over the phone and must be complied with within one month.

In cases where someone asks you for their personal information over the phone write down the relevant detail and ask them if they are willing to put the request in writing. Remember they don't have to put the request in writing so if they refuse the phone request is sufficient. It is therefore very important that you take down as much detail about the request as possible.
Further details about the Subject Access Request process can be found on the SiP.

## 21. Authorised Users

Authorised users will only have access to personal information where that access is essential to their duties. Authorised users should discuss with their line manager any instance where access rights require clarification. Access rights are not to be regarded as permanent and are subject to change at any time depending upon the nature of the duties being fulfilled by the authorised user.

Authorised users with access to personal information must be familiar with the requirements of the General Data Protection Regulation 2016 and familiar with the content of this policy.

Authorised users should only record information about an individual which is relevant, and should be aware that they may be required to justify what has been written and be prepared for that information to be released as part of a subject access request.

Any authorised user who is found to have inappropriately divulged personal information will be subject to investigation under the School's disciplinary procedure, which may result in dismissal and possible legal action.

All authorised users must follow good practice as indicated by the GDPR and any such codes of practice issued by the Office of the Information Commissioner or the School, when processing personal data.

## 22. Direct Marketing

The School will not participate in direct marketing practices in the absence of:

- Explicit consent from the data subject
- A legitimate interest reason – Officers must conduct a balancing exercise before seeking to rely on a legitimate interest reason.

Even where legitimate interests or explicit consent has been established, all correspondence and the relevant webpages must include opt-out options.

All individuals must be given the opportunity to opt-in to receive material at the point of data collection.

The appropriate opt-in mechanisms must be put in place where third party marketing or advertising materials are distributed to named individuals. In situations where this cannot be feasibly done, the materials must not be distributed.

## 23. Our responsibilities

By following and maintaining strict safeguards and controls, the School has to:

- designate a Senior Information Risk Owner responsible for information risk within the authority.

- have an Information Governance Team or support service available to them responsible for gathering and distributing information and issues relating to information security, the GDPR and other related legislation.
- have a designated departmental Information Asset Owner, responsible for issues relating to information security and the GDPR within their own department
- make sure that all activities that relate to the processing of personal data have the correct safeguards and controls to make sure of information security and compliance with the GDPR.
- make sure that all contracts and service level agreements (SLA) between the School and external organisations, including contract staff refers to the GDPR where necessary and is logged onto our contracts registered and is monitored.
- work towards adopting, as best practice, the key principles of ISO 27001 & ISO 17799 – the International Standard for Information Security.
- Ensure that all staff are fully aware of the content of this policy and handle personal data in line with this policy.
- Ensure all staff have training in relation to information governance and data protection.

## 24. Responsibilities of all staff

- Fully understand your data protection obligations
- Check that any data processing activities you are dealing with comply with our policy and are justified
- Do not use data in any unlawful way
- Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions
- Comply with this policy at all times
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay
- Managers are responsible for ensuring that this policy is communicated to all employees including temporary staff and that it is adhered to. It must be communicated to all contractors, agents and partners working for or on behalf of the School.
- All authorised users must ensure that any request for information they receive is dealt with in line with the requirements of the GDPR and that they comply with this policy.
- Managers are responsible for ensuring all employees complete the mandatory DPA training.
- All elected members, contractors, agents and partners working for or on behalf of the Council must complete the mandatory DPA training.

## 25. Compliance with the Data Protection Policy

The Governing Board is responsible for monitoring compliance with this policy.

If employees knowingly do not comply with School's policies, procedures or guidelines, the Council may take appropriate action in accordance with the Employee Code of Conduct.

## 26. Other Relevant Policies, Standards and Procedures

These can be found on the SiP or contact Derby City Council's Information Governance Team on: data.protection@derby.gov.uk.

## 27. Contact Details

Please contact the Information Governance team with enquiries about this or any other referenced policy, procedure or law.

Email to: data.protection@derby.gov.uk
Telephone: 01332 640763

## Appendix 1

Definitions

| | |
|---|---|
| **Personal data** | 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.<br>*Personal data we gather may include: individuals' phone number, email address, educational background, financial and pay details etc.* |
| **Special categories of personal data** | Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information |
| **Data controller** | 'Data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law. |
| **Data processor** | 'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. |
| **Processing** | 'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or |

| | |
|---|---|
| | combination, restriction, erasure or destruction. |
| **Supervisory authority** | This is the national body responsible for data protection. The supervisory authority for our organisation is the Information Commissioners Office. |