Repton Primary School

Data Protection Policy

Version 1

Last Reviewed	**Feb 2021 – 03/010221**
Reviewed By	**Governors**
Next Review Date	

Contents

1.1 Introducing our DP Policy 4
1.2 Scope and Responsibilities 4
1.3 DP Legislation & Regulator 4
1.4 Our DP Objectives 4
1.5 Our DP Rules 5
1.6 Rights: 6
1.7 Data sharing 8
1.8 Non-EEA data transfers 8
1.9 Data protection breaches 8
Annexe.1 Legal Conditions for Processing 9
A1.1 Introduction 9
A1.2 Our role and bases for processing 9
A1.3 Data Subjects' Rights 10
Annexe.2 Data Protection - Personal Data Breach Procedure 11
A2.1 Introduction 11
A2.2 Scope and Responsibilities 11
A2.3 What is a Personal Data Breach? 11
A2.4 Becoming Aware of a Breach 11
A2.5 Breach Response Plan 11
A2.6 Data Breach Checklist 15
Annexe.3 Data Protection Impact Assessment Guidance and Template 16
A3.1 Introduction 16
A3.2 What is a Data Protection Impact Assessment (DPIA)? 16
A3.3 When will a DPIA be appropriate? 16
A3.4 The Benefits of a DPIA 16
A3.5 Steps to be followed when considering a new project 17
A3.6 Monitoring 17
A3.7 Template Data Protection Impact Assessment Form 18

Annexe.4 Subject Access Request (SAR) Procedure 26

A4.1 Introduction 26

A4.2 Scope and Responsibilities 26

A4.3 Receiving a valid SAR 27

A4.4 Responding to a SAR 27

A4.5 Exemptions 28

A4.6 SAR Request Form 29

Annexe.5 Freedom of Information requests under the Freedom of Information Act 2000 32

A5.1 Introduction: what a publication scheme is and why it has been developed 32

A5.2 Values 32

A5.3 Categories of information published 32

A5.4 How to request information 32

A5.5 Paying for information 33

A5.6 Classes of Information Currently Published ..... **Error! Bookmark not defined.**

A5.7 Feedback and Complaints 33

1.1 Introducing our DP Policy

1. Our Data Protection (DP) Policy lays out our approach to data protection. We recognise the importance of protecting the personal data we are entrusted with, and this policy sets out how we comply with relevant legislation.
2. If you have any queries about this Policy, please contact [our Data Protection Officer], whose details can be found in our Privacy Notices.

1.2 Scope and Responsibilities

This Policy applies to all staff, including temporary staff, consultants, governors, volunteers, and contractors, and anyone else working on our behalf.

All staff are responsible for reading and understanding this policy before carrying out tasks that involve handling personal data, and for following this policy, including reporting any suspected breaches of it to our Data Protection Officer.

All leaders are responsible for ensuring their team read and understand this policy before carrying out tasks that involve handling personal data, and that they follow this policy, including reporting any suspected breaches of it.

Our Data Protection Officer is responsible for advising us about our data protection obligations, dealing with breaches of this policy, including suspected breaches, identified risks, and monitoring compliance with this policy.

1.3 DP Legislation & Regulator

1.3.1 Relevant legislation includes:

- General Data Protection Regulation (GDPR);
- Data Protection Act 2018 (DPA 2018), which enacts the GDPR in the UK and includes exemptions and further detail, as well as offences that individuals can be prosecuted for;
- Privacy and Electronic Communications Regulations (PECR), which cover electronic direct marketing ("marketing" includes fundraising and promoting an organisation's aims, not just selling.)
- Freedom of Information Act 2000, which provides key definitions referred to in the other legislation.

1. In the UK, the Information Commissioner's Office (ICO) is the data protection regulator.
2. Breaches of data protection legislation can result in significant monetary penalties and damage to reputation, as well as the risk of real harm to people whose data is handled in an unfair or unlawful way. Individual members of staff may be prosecuted for committing offences under Sections 170 – 173 of the DPA 2018.

1.4 Our DP Objectives

We are committed to making sure that:

1.4.1 Personal data is only processed in keeping with legal data protection principles. The principles include: data being processed lawfully, fairly and in a transparent manner; data being processed only

for specific, explicit and legitimate purposes; data being adequate, relevant and accurate,; data not being kept longer than is necessary; and data being kept secure;

1.4.2 We adopt a "Privacy by Design" and "Privacy by Default" approach;

1.4.3 We can demonstrate our accountability and compliance;

1.4.4 The people whose data we hold (Data Subjects) understand the ways and reasons why we process their data, and can easily and fairly exercise their rights around their data;

1.4.5 We only share personal data when it is fair and lawful to do so, and when we share data we do it in a safe and secure way;

1.4.6 Data is not transferred outside of the European Economic Area (EEA) except where the EU has made an 'adequacy decision' or the transfer is covered by 'appropriate safeguards', as defined in GDPR Article 44;

1.4.7 All data breaches, including near misses, are managed properly and reported appropriately, so we can minimise any risks and improve practices in the future. This includes any breaches of the Data Protection Act (DPA 2018) where the individual responsible may be liable.

1.5 Our DP Rules

1.5.1 We follow the legal Data Protection Principles:

i. **Fair, lawful and transparent processing:** The reason for processing of personal data must meet one of the legal conditions listed in Article 6 of the GDPR, and when "special categories" of personal data are being processed, the purpose must also meet one of the legal conditions listed in Article 9 of the GDPR. "Special categories" are information about a person's race or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health, genetic and biometric data, sexual life or sexual orientation.

Legal conditions: See Annexe 1 for an explanation of the Legal Conditions for Processing.

Other legislation: All processing must also comply with the other DP Principles and any other relevant legislation, including the DPA 2018 and the Privacy and Electronic Communications Regulations (PECR) as appropriate. Any individual who obtains, discloses or retains data when they do not have permission to do so may be committing an offence under the DPA 2018 Section 170. All electronic "direct marketing" is subject to the PECR, which require us to obtain consent before sending direct marketing messages electronically.

Transparency: To be fair and transparent, our data processing, including how and why we process data, is explained in our Privacy Notices. We also explain how and why data will be processed at the point where we collect that data, as much as is reasonably possible, and especially if the processing is likely to be unexpected.

ii. **Purpose limitations:** We only use the data we collect for the reasons we explained in our privacy notice. If we need to use it for another reason, we will inform our data subjects of the new reason for processing before we do it.

iii. **Data limitations:** We minimise the amount of data that we collect and process, keeping it to only what is necessary for the reasons we are collecting it. We should never collect or keep any personal data "just in case".

iv. **Data accuracy:** We will always try to make sure the data we collect and hold is accurate, and keep it up to date as appropriate.

v. **Data retention:** We will only keep personal data for as long as is necessary for the reasons for which we are processing it, and we will be transparent with our data retention schedules which can be found

on Repton Primary Schools website under GDPR. Any individual who purposefully retains data that they do not have permission to be holding, may be committing an offence under the DPA 2018 Section 170.

vi. **Data security & integrity:** We use both technical and organisational security measures to protect data from unauthorised or unlawful processing, or from accidental loss, destruction or damage. Security measures should be appropriate to the level of risk involved in the data and the processing. Our measures include, but are not limited to: technical measures such as ICT systems security, ICT access controls, pseudonymisation, and encryption; and organisational measures such as business continuity plans, physical security of our premises and data, policies, procedures, training, audits and reviews.

Security should be considered at all times. This includes when data is being stored, used, transferred, or disposed of, whether the data is electronic or hard copy, and regardless of how and where the data is being accessed and stored, especially when data is sent or taken off site, or to another organisation. Emails & MS Teams Chat/Data is automatically deleted 18 months after receipt/being sent.

Any individual who purposefully re-identifies pseudonymised information without permission may be committing an offence under the DPA 2018 Section 171.

1.5.2 Privacy by Design & Default : Wherever possible, we adopt a Privacy by Design & Default approach. When we are planning projects or new ways of working that involve processing of personal data, we will consider the data protection implications, and how to make sure we meet legal and good practice requirements, from the planning stages, and keep a record of the outcomes.

For particularly high-risk processing, whether from a new or adapted way of working with personal data, we will do this using Data Protection Impact Assessments (DPIAs), to document the risks, decision-making process and decisions made, including recommendations and actions.

High risk processing includes processing the data of children under Article 35(3) as children are vulnerable data subjects and the data processed is often sensitive or highly personal data.

A DPIA may be carried out to decide if any changes or new controls are needed for existing ways of working.

1.5.3 **We Demonstrate our Accountability:** To demonstrate and support our compliance with data protection legislation, we keep records of the processing we carry out, we have appropriate policies and procedures in place, we train our staff in data protection, we have a Data Protection Officer in post, we carry out regular audits and reviews of our activities, and we record and investigate data security breaches.

Our records of processing include our contact details and information about why we are processing personal data, what types data we process, the categories of people we process data about, information about how long we hold the data for, and general information about our security measures, as well as the types of external the data is shared with, including any transfers outside of the EEA, and the safeguards in place if data is transferred outside the EEA.

1.6 Rights:

We process personal data in line with the legal rights of data subjects', including their right to:

- Be informed about their data being processed, which links to the first DP Principle of fair, lawful and transparent processing;
- Request access to their data that we hold (sometimes requests are known as [Data] Subject Access Requests, or DSARs or SARs);

- Ask for inaccurate data to be rectified;
- Ask for data to be erased (sometimes known as the “right to be forgotten”);
- Restrict processing of their data, in limited circumstances;
- Object to the processing, in some circumstances, including stopping their data being used for direct marketing;
- Data portability, which means to receive copies of some of their data in a format that can be easily used by another organisation or person;
- Not be subject to automated decision making or profiling, if it has legal effects or similarly significant effects on the data subjects;
- Withdraw consent when we are relying on consent to process their data;
- Make a complaint to the ICO or seek to enforce their rights through the courts.

We will respond to, and fulfil, all valid requests within one calendar month, unless it is necessary to extend the timescale, by up to two months in certain circumstances. Not all the rights are absolute rights, and we cannot always carry out the requested action in full, or at all. For example, the right to erasure may be limited in some circumstances because we are required to keep some records, and a number of exemptions in the DPA 2018 apply to SARs, meaning we can withhold some information in some situations.

In responding to requests we also explain to data subjects they have the right to make a complaint to the ICO or seek to enforce their rights through the courts.

Any individual who purposefully alters, defaces, blocks, erases, destroys or conceals information to prevent it being provided to a data subject who has requested it, and has a right to receive it, may be committing an offence under the DPA 2018 Section 173.

1.7 Data sharing

1.7.1 Data Processors:

We rely on the services of a number of external to support our work (both management and curriculum). These may include people, companies, systems and software that process personal data as part of the work they do on our behalf. These are our "data processors". When working with data processors, we will carry out appropriate due diligence checks to make sure that they can provide sufficient guarantees that they will comply with data protection legislation, including keeping data secure and cooperating with us to uphold data subjects' rights. We will require contractors and their staff to comply with this DP Policy.

We will appoint data processors only on the basis of a legally binding, written contract, that requires them to, amongst other things: only process personal data based on our instructions; keep the data secure; assist us to comply with our legal obligations and uphold data subjects' rights; delete or return the data at the end of the contract; and allow inspections and audits of their processing activities. Data Processor contracts, and compliance, will continue to be monitored throughout the contract period.

1.7.2 Third Parties:

We will only share personal data with any other external, including other data controllers such as agencies and organisations, when the sharing meets one or more appropriate legal condition, and is carried out in keeping with the data protection principles and while upholding the rights of data subjects. Where necessary we will enter into Data Sharing Agreements (DSA), or similar agreements, to help facilitate the sharing of personal data. A DSA does not make the sharing lawful, it only provides a framework to work within, to help share data in an effective and safe way that respects people's data protection rights, when an appropriate and lawful reason to share the data has been identified.

1.8 Non-EEA data transfers

Personal data will not be transferred outside the EEA unless it is allowed by the conditions in Chapter V of the GDPR. This includes storage of data on cloud-based servers that are located outside the EEA.

1.9 Data protection breaches

All breaches, or suspected breaches, of this policy will be reported immediately to the Data Protection Officer, and will be investigated appropriately, corrective and preventive action taken and recorded. This includes, but is not limited to, any personal data we handle being lost, or being shared, destroyed, changed or put beyond use when it shouldn't be.

Specifically, breaches that are likely to result in a risk to the rights and freedoms of data subjects, will be reported to the ICO within 72 hours of the school becoming aware of the breach.

If a breach is likely to cause a high risk to affected data subjects, we will also tell the data subjects, as soon as possible and without undue delay, to allow them to take any actions that might help to protect them and their data. We will also consider informing data subjects about a breach, even if there is not a likely high risk, if it is an appropriate step for other reasons, such as preserving open communication.

We will log all breaches, including those that are not reportable to the ICO.

Annexe.1 Legal Conditions for Processing

A1.1 Introduction

"Personal data" means **any** information where a living person is either identified or identifiable, from the information alone, or with other information. Personal data can include written information, pupil work, photographs, CCTV and film footage or voice recordings, in electronic format (which can include in Social Media, apps, databases or other electronic formats) or hard copy (including copies printed from electronic sources, and handwritten data when it is part of a filing system, or intended to be filed).

"Special category data" is personal data that needs more protection because it is sensitive.

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

In addition, the DfE advises that Pupil Premium/FSM status is treated as Sensitive Data

"Data Subjects" include our pupils, staff, contractors, parents, local authority contacts, and anyone else we might come into contact with.

"Data Controller" means the school, alone or jointly with other Data Controllers, decides on why and how personal data is processed.

"Processing" means collecting, storing, using, sharing and disposing of data.

"Processors" are the external bodies who processes personal data on behalf of the controller.

A1.2 Our role and bases for processing

The role of any school is to educate and safeguard children. These are statutory obligations and come from various Acts and statutory instruments that can be found here.

This means the overwhelming volume of our collection and processing data is covered under Article 6 (1) c of the General Data Protection Regulations 2018: processing is necessary for compliance with a legal obligation to which the controller is subject:

Equality Act 2010
Education (Governors' Annual Reports) (England)(Amendment)Regulations 2002.
Special Educational Needs and Disability Act2001
Health & Safety of Pupils on Educational Visits 1998
Safeguarding Vulnerable Groups Act 2006
Disability Discrimination Act(s)
The Education Act 1944, 1996, 2002, 2011
The Education & Adoption Act 2016
The Education (Information About Individual Pupils) (England) Regulations 2013
The Education and Skills Act 2008
The Education (Pupil Registration) (England) Regulations 2006
Statutory Guidance for Local Authorities in England to Identify Children Not Receiving Education – February 2007)
The Education and Inspections Act 2006

The Children Act 1989, 2004
The Childcare Act 2006
The Children & Families Act 2014
Local Safeguarding Children Boards Regulations 2006 (SI 2006/90)
The Localism Act 2011 Contract (traded services)

Some of our functions in educating and safeguarding children that cannot be directly linked to a statutory function above may be carried out under Article 6 (1) e of the General Data Protection Regulations 2018: processing is necessary for the performance of a task carried out in the public interest.

Where we process special category data, we do so under the General Data Protection Regulation Article 9(2g) - Processing is necessary for reasons of substantial public interest

Data Protection Act 2018 part 2 schedule 1;

8 - Equality of Opportunity or Treatment

16 - Support for Individuals with a Particular Medical Condition

18 - Safeguarding Children and Individuals at Risk.

When we wish to process data for any other reason, we will ask for parental / pupil (where appropriate) consent as per Article 6 (1) a of the General Data Protection Regulations 2018. Typically this will be for areas of our work that includes the public celebration of our school and pupils' work. Parents / children (where appropriate) retain the right to change their consent preferences at any time by notifying the school office.

A1.3 Data Subjects' Rights

All of our data subjects have a number of rights – these are detailed in 1.6 above.

To exercise these rights or for further help and information about processing and our commitment to keeping data safe, please contact our Data Protection Officer:

Data Protection Officer:
GDPR for Schools, Derbyshire County Council
Room 396, North Block
County Hall
Smedley Street
Matlock
Derbyshire
DE4 3AG
gdprforschools@derbyshire.gov.uk
01629 532888

Annexe.2 Data Protection - Personal Data Breach Procedure

A2.1 Introduction

A2.1.1 We recognise that a breach of personal data could happen, despite our policies, procedures and measures in place to protect personal data, and we will respond to any breach as quickly as possible in order to minimise any risks or potential harm, to the school or to individuals.

A2.1.2 This procedure supports our Data Protection Policy. It includes our guidelines for reacting to and handling any breach, or suspected breach, or personal data, in line with the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA 2018) and best practice.

A2.2 Scope and Responsibilities

This policy applies to all instances when it is known or suspected that personal data that the school handles has been subject to a breach (see below for breach definition.)

All staff are responsible for reading, understanding and complying with this policy.

Our Data Protection Officer provides assistance and further guidance on data breaches. The Head Teacher is responsible for taking the lead on the steps in this procedure once a breach, or suspected breach, has been reported internally, including reporting to the Data Protection Officer.

A2.3 What is a Personal Data Breach?

A2.3.1 If personal data we handle is lost, destroyed, altered, disclosed, accessed or put beyond use when it shouldn't be, this is a Personal Data Breach. This procedure will be followed **as soon as** we become aware of a breach.

A2.3.2 Where we suspect personal data has been subject to a breach, we will follow this procedure until we are sure of the status of the personal data.

A2.3.3. A personal data breach can occur accidentally or intentionally, by staff, or anyone else.

A2.4 Becoming Aware of a Breach

Any staff member becoming aware of a breach is responsible for immediately reporting it internally, to ensure it can be handled appropriately.

A2.5 Breach Response Plan

All members of staff are responsible for taking all reasonable steps and cooperating with key staff in following this procedure when a breach is found or suspected.

The breach response plan has 8 steps, which are covered in detail below:

1. Report the breach internally;
2. Record the breach (using the GDPRiS software where applicable)
3. Assess the risk;
4. Contain and recover;
5. Notify the ICO of the breach (if applicable);
6. Notify the affected Data Subjects of the breach (if applicable);

7. Review.
8. Implement any necessary changes to prevent reoccurrence.

Use the Data Breach Checklist (at the end of this procedure) and Data Breach Log for all personal data breaches.

A2.5.1 Report the breach internally (school staff)

As soon as you become aware of a breach, or possible breach, report it to the Head Teacher or the Deputy Head Teacher in their absence, who will lead on the breach response, and inform the Data Protection Officer of the breach and keep them updated on the investigation and actions as appropriate.

The report should be made as soon as possible even if the breach is discovered outside of normal working hours.

A2.5.2 Record the breach (school staff)

Log the breach (using the GDPRiS software where applicable). Include as many details as possible and attach documents or evidence if appropriate.

A2.5.3 Assess the risk (DPO)

Consider what harm could come from the breach, including who could be harmed, how they could be harmed, and how severe the harm could be, as well as how likely is the harm to happen. This risk assessment, based on severity and likelihood, will depend on the types of information involved (how sensitive is it, what could be done with it?), how much information is involved, and how exposed the data is, as well as the individual circumstances of the data subjects (people the data is about.)

As an example regarding exposure, if a laptop has been lost, if it is encrypted there is a very small chance of any data being accessed. But if hard copy documents have been lost or left unattended, they are much more likely to be accessed and read.

As another example, if personal data is included in an email by accident, the data may be at more risk of being misused if the email has gone to a member of the public, rather than to another school.

As an example regarding the data subjects' circumstances, accidentally disclosing an address might not pose a risk to most data subjects, but it could be very high risk for someone who is escaping domestic violence, or for the adoptive family of a child.

A2.5.4 Contain and recover (School with DPO support)

Take reasonable actions to contain the risks, and/or recover the data, if possible.

Containment and recovery actions could include, as appropriate:

- Attempting to find lost devices or paperwork;
- If devices have been stolen, report this to the police;
- If a breach is still occurring, for example, due to an ongoing IT issue, then IT should take appropriate steps to minimise the breach, such as closing down an IT system. In the event of a Cyber attack, immediately report to the Action Fraud line on 0300 1232040.
- Warning staff and third parties such as the County Council, to be aware of any "phishing" attempts that might be linked to personal data that has been accessed by criminals/unauthorised people;
- If data has been sent to, or shared with, someone it shouldn't have been, consider if you can contact them to recover the data. Bear in mind that "recall" doesn't usually work on externally sent emails;
- If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use;

- If the data breach includes any entry codes or IT system passwords, change these immediately and inform the relevant agencies and members of staff;
- Contacting the County Council's Communications Division if part of the crisis service, so that they can be prepared to handle any press enquiries. The Council's Senior Communications Officer can be contacted by telephone: 01629 538234.

A2.5.5 Notify the ICO of the breach (DPO);

Breaches that could cause a risk to people should be reported to the Information Commissioner's Office (the ICO – the UK's data protection regulator) and, in some cases, to the data subject(s) involved too.

Not all breaches will need to be reported. For example, if data is deleted in error it is *technically* a breach, but if the data is backed up and can be promptly reinstated, it does not represent a risk to data subjects.

If the DPO decides not to report a breach to the ICO and/or the data subjects involved, the decision and reasons will be recorded.

If it is likely the breach will result in a risk to people's rights and freedoms, and have an adverse effect on data subjects, causing them harm, it must be reported to the ICO.

Reports to the ICO must be made within 72 hours of us becoming aware of the breach. Information can be provided to the ICO in stages, giving them the details as and when we find out more, but the first contact must be within 72 hours.

The information to be provided to the ICO:

- A description of the personal data breach that has occurred including, where possible:
  - The types and approximate number of people whose data is involved;
  - The types and approximate number of personal data records involved;
- The likely consequences of the breach;
- The measures taken, or proposed to be taken, in response to the breach, including actions to mitigate any possible harm to data subjects;
- The name and contact detail of the Data Protection Officer, or any other contact details of people who can provide more information.

Guidance on how to report to the ICO is on their website: https://ico.org.uk/for-organisations/report-a-breach/

A2.5.6 Notify the affected Data Subjects of the breach (DPO);

If the risk to data subjects is assessed as high, the breach must also be reported to everyone whose data is involved, to allow them to take any appropriate steps to protect themselves and so they are aware of anything that may happen. For example, if financial information has been lost or stolen, they can alert their bank for fraudulent activity, or if passwords have been lost or stolen they can change them on their accounts and any other accounts that they used the same password on.

We can choose to report to data subjects even if the risk is not high, if we consider it would be better for us to tell them about the breach for other reasons, such as supporting transparent relations and trust.

A2.5.7 Review

The review stage includes reviewing and evaluating the response to the breach. Consider how effective the response was, and if improvements could be made when handling any future breaches.

As examples, did the person who first became aware of the breach know to report it internally? Did attempts to recover the data work? How could the breach have been handled better or quicker?

The breach, and outcomes of the review, should be reported to the next available Senior Management Team and Full Governors meeting for discussion. If systemic or ongoing problems are identified, then an

action plan will be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation will liaise with Human Resources or Internal Audit for advice and guidance.

A2.5.8 Implement any necessary changes to prevent reoccurrence.

Depending on how the breach occurred, actions should be taken to reduce the risk of something similar happening, including amongst other things, improved IT security, new or improved written procedures, refresher training, improved supervision, changes to processes, communications to remind colleagues about risks, etc.

A2.6 Data Breach Checklist

Action	**Taken? Give dates, initials and links to docs where appropriate**
Date and time of discovery	
Date and time of occurrence	
What happened	
Immediate steps taken to contain the breach, e.g. changing passwords, shutting computers down, halting network traffic, restore data from backups	
Acknowledge breach by thanking informant for information – log it here	
Inform DPO	
Assess Risk:	[Consider how many people are affected, what type of data is involved, how could people be harmed, and how likely are they to be harmed?]
Necessary to inform ICO? 0303 1231113	
Date and time reported to ICO	
Necessary to inform data subjects?	
Data subjects informed?	
Police informed?	
Review:	[Consider what was in place that should have prevented the breach, and why it failed, how could further breaches be prevented, how have we helped the people effected? Should we improve security, procedures, training, etc?]
Steps taken to avoid reoccurrence	
Concluding letter	
SLT / Governors de brief	
Report completed by	

Annexe.3 Data Protection Impact Assessment Guidance and Template

A3.1 Introduction

A Data Protection Impact Assessment (DPIA) is a tool which can help Repton Primary School identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.

An effective DPIA will allow the school to identify and fix problems at an early project stage, reducing the associated costs and damage to reputation which might otherwise occur.

This procedure explains the principles which form the basis for a DPIA, sets out the basic steps which the School should carry out during the assessment process and includes a template which can be adapted as needed to fit the project.

DPIAs should be drawn up with the assistance of the DPO, who will have the expertise needed to fully consider the issues.

A3.2 What is a Data Protection Impact Assessment (DPIA)?

A DPIA is a process which helps an organisation to identify and reduce the privacy risks of any project which involves personal data. To be effective a DPIA should be used throughout the development and implementation of the School's project.

A DPIA will enable the School to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved, as well as provide evidence of investigation into the suitability of any third parties who will be given access to data in the project.

A3.3 When will a DPIA be appropriate?

DPIAs should be considered for all new projects, because this allows greater scope for influencing how the project will be implemented. A DPIA can also be useful when planning changes to an existing system.

The school **must** carry out a DPIA for processing that is likely to result in a "high risk to individuals" (Article 35(1) GDPR). When considering if the processing is likely to result in high risk, the School and the DPO should consider the relevant European guidelines. These define nine criteria of processing operations that are likely to result in high risk. The two most relevant to schools relate to processing of vulnerable data subjects (children) and the processing of Sensitive data or data of a highly personal nature. Because many new projects in schools include the processing of children's data including Sensitive data, it is likely that most projects in schools will require a DPIA to be carried out.

Conducting a DPIA does not have to be complex or time consuming but there must be a level of rigour in proportion to the privacy risks arising.

A3.4 The Benefits of a DPIA

Consistent use of DPIAs will increase the awareness of privacy and data protection issues within the School and ensure that all relevant staff involved in designing projects think about privacy at its earliest stages.

Examples of where a DPIA would be appropriate

- A new IT system for storing and accessing personal data.
- A data sharing initiative where two or more schools seek to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new database which consolidates information held by separate parts of the school.
- Legislation, policy or strategies which will impact on privacy through the collection or use of information, or through surveillance or other monitoring.
- Cloud hosted applications.
- The collection of new data on an existing system.

A3.5 Steps to be followed when considering a new project

A DPIA should be undertaken before a project is underway, in the same way that schools consider the cost impact of a project before making a commitment to spend any money. Consultation should be made with the DPO and consideration should be given to consulting with affected data subjects as a first step. The DPIA process should then be a collaborative task between the Headteacher, Business Officer and staff who will be using the system/managing the project under consideration.

A3.6 Monitoring

The completed DPIA should be checked and approved by the DPO and then submitted to the Governing Body for final review and approval. The Governing Body will monitor implementation of actions identified in DPIAs.

A3.7 DATA PROTECTION IMPACT ASSESSMENT FOR [NAME OF PROJECT]

Name of School:
Date:
Document prepared by:

** THIS IS A DRAFT TEMPLATE REQUIRING ONGOING ADAPTATION BY THE SCHOOL **

IF YOU IDENTIFY A HIGH RISK THAT CANNOT BE MITIGATED, YOU MUST CONSULT WITH THE ICO. YOUR DPO WILL ADVISE ON THIS.

Version History			
Version	**Date**	**Detail**	**Author**
1.0	12/12/19	Template	GDPR in Schools, Derbyshire County Council

Approved by DPO DATE:

Approved by Governors DATE:

Introduction

Description of project

Screening questions

- Will the project involve the collection of new information about individuals? If yes, please detail the information to be collected.
- Will the project compel individuals to provide information about themselves? If yes, please detail the information to be provided.
- Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? If yes, please detail which organisations will be provided with access.
- Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? If yes, please describe the new purpose below.
- Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition. If yes, please detail the new technology.
- Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them? If yes, please describe the impact, below.
- Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private. If yes, please describe the information to be collected, below.
- Will the project require you to contact individuals in ways that they may find intrusive? If yes, please describe how the individuals will be contacted, below.

[Include Notes regarding Consultation]

Step one: Identify the need for a DPIA

What does the project aim to achieve?

What will the benefits be to the organisation, to individuals and to other parties?

Organisational benefits	Individual benefits	Other party benefits

Why was the need for a DPIA identified?

How many individuals are likely to be affected?

How will data be collected, used, amended and deleted?

If sensitive personal data is involved, have you established how this will be handled, accessed, retained and disposed of?

What practical steps have been taken to ensure that risks to privacy have been identified and addressed?

Is information quality good enough, how will data be verified & recorded accurately?

What security and/or information risks have you identified?

Have training and instructions been given to appropriate staff to ensure compliance with policy and procedure?

What process is in place to answer Subject Access Requests in relation to the data held under the new project?

Step two: Describe the information flows

Complete a word or pictorial description of the information flow as appropriate.

Step three: Identify the privacy and related risks

Privacy Issue	Risk Rating	Risk to Individuals	Compliance risk	Organisational risk

Step four: Identify privacy solutions and sign off and record the DPIA outcomes

Risk	Solution(s)	Risk Rating after solution applied

Risk Rating Decision

As a result of the privacy risks and mitigations it has been evaluated that the overall level of residual risk to privacy for the use of this software stands at Level X [Low/Medium/High or figure based on risk rating table which may be included] This is/is not a high risk and therefore we do/do not need to consult with the ICO.

Step five: Integrate the DPIA outcomes back into the project plan

Who is responsible for integrating the DPIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action To be Taken	Date of completion	Responsibility for
Adapt and amend this Template DPIA to fit the requirements of the individual school		
Consult with DCC GDPR team, DPO and Governors		
Approval of the final version of this DPIA by DPO		
Update information asset register/map		
Amend Privacy Notice(s)		
Amend relevant policies e.g. IT Policy and Acceptable User Agreement, Safeguarding and Child Protection Policy [any others relevant to individual school]		
Establish regular review of this DPIA and the function of the project		
[Insert other actions relevant to project]		

Appendix A: Evidence of due diligence of supplier (if relevant)

Appendix B: Supplier Contract

To be added by school if relevant

Appendix C: Linking the DPIA to the Data Protection Principles

Answering these questions during the DPIA process will help you to identify where there is a risk that the project will fail to comply with the GDPR or other relevant legislation, for example the Human Rights Act.

Principle 1

Lawfulness, fairness and transparency of data processing

There must be lawful basis for processing the personal data as follows;

(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. (This cannot apply if you are a public authority processing data to perform your official tasks.

Have you identified the purpose of the project and which lawful basis applies?	a/b/c/d/e/f
Is the processing of the data necessary in terms of GDPR?	Y/N
How will you tell individuals about the use of their personal data?	P.N.
Do you need to amend your privacy notices?	Y/N
If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?	
If special categories of personal data have been identified have the requirements of GDPR been met?	Y/N
As the School is subject to the Human Rights Act, you also will, where privacy risk are especially high, need to consider:	
Will your actions interfere with the right to privacy under Article 8	Y/N
Have you identified the social need and aims of the project?	Y/N
Are your actions a proportionate response to the social need?	Y/N

Principle 2

Personal data shall be obtained only for one or more specified explicit and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Does your project plan cover all of the purposes for processing personal data?	Y/N
Have you identified potential new purposes as the scope of the project expands?	Y/N
Does your Privacy Notice cover all potential uses?	Y/N

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Is the quality of the information good enough for the purposes it is used?	Y/N
Which personal data could you not use, without compromising the needs of the project?	

Principle 4
Personal data shall be accurate and, where necessary, kept up to date.

If you are procuring new software does it allow you to amend data when necessary?	Y/N
How are you ensuring that personal data obtained from individuals or other organisations is accurate?	

Principle 5
Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary.

What retention periods are suitable for the personal data you will be processing?	
Are you procuring software that will allow you to delete information in line with your retention periods?	Y/N

Principle 6
Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Do any new systems provide protection against the security risks you have identified?	Y/N
What training and instructions are necessary to ensure that staff know how to operate a new system securely?	

Rights of Data Subjects and Privacy by Design

Will the systems you are putting in place allow you to respond to subject access requests more easily?	Y/N
Will the system allow compliance with individual rights under GDPR, in particular the right to be informed, the right to rectification and the right to ensure (right to be forgotten).	Y/N
If the project involves marketing, have you got a procedure for individuals to opt in to their information being used for that purpose?	

Transferring data outside European Economic Area
Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data**.**

Will the project require you to transfer data outside of the EEA?	Y/N
If you will be making transfers, how will you ensure that the data is adequately protected?	Y/N

Annexe.4 Subject Access Request (SAR) Procedure

A4.1 Introduction

A4.1.1 We process personal data in line with all of the legal rights of data subjects', including their right to:

- Be informed about their data being processed, which links to the first DP Principle of fair, lawful and transparent processing;
- Request access to their data that we hold;
- Ask for inaccurate data to be rectified;
- Ask for data to be erased (sometimes known as the "right to be forgotten");
- Restrict processing of their data, in limited circumstances;
- Object to the processing, in some circumstances, including stopping their data being used for direct marketing;
- Data portability, which means to receive copies of some of their data in a format that can be easily used by another organisation or person;
- Not be subject to automated decision making or profiling, if it has legal effects or similarly significant effects on the data subjects;
- Withdraw consent when we are relying on consent to process their data;
- Make a complaint to the ICO or seek to enforce their rights through the courts.

A4.1.2 This procedure supports our Data Protection Policy, and explains how we respond to requests from, or on behalf of, individuals for access to the data we hold that is about the individual. This is known as the right to access, and is a legal right under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018). Requests are known as [Data] Subject Access Requests, or DSARs or SARs.

A4.1.3 In addition, pupils, or parents on their behalf, have the right to access curricular and educational records relating to the pupil, under the Education (Pupil Information) (England) Regulations 2005 (EPIR 2005).

A4.1.4 To exercise any of the rights above, contact our Data Protection Officer.

A4.2 Scope and Responsibilities

The right to access applies to all pupils, parents, staff and anyone else that we hold personal data about. In some circumstances, for example with pupils, a parent or other person with authority may make the Subject Access Request on their behalf.

All staff are responsible for reading and understanding this procedure if they may receive a SAR on behalf of the school, as SARs can be made through any member of staff, although responses should be centrally coordinated. All leaders are responsible for ensuring their team read and understand this procedure if they may receive a SAR on behalf of the school.

Our Data Protection Officer (DPO) provides assistance and further guidance on responding to SARs, and coordinates all responses.

Any individual who purposefully alters, defaces, blocks, erases, destroys or conceals information to prevent it being provided to a data subject who has requested it, and has a right to receive it, may be committing an offence.

A4.3 Receiving a valid SAR

Format: A SAR does **not** need to be in writing, it can be in any format, including a letter, email, text message, over social media, over the telephone, or face to face, and can be made to any representative of the school.

However, in order to process the request as efficiently as possible, and to help us comply with statutory timeframes, we ask that the form contained in Annexe 1 below is completed.

Content: A SAR does **not** need to refer to data protection legislation or be described as a subject access request. Any request for access to personal information from, or on behalf of, a data subject, should be treated as a SAR.

Identity & Authority: We must verify the identity of the person making the SAR, and if the SAR is being made on behalf of someone else, we must confirm they have authority to act on their behalf in exercising their rights. Checking identity should not be used as a delaying tactic, and how to verify identity will depend on who is making the SAR, and how well they are known to the person handling the request. For example, a staff member will not usually be required to confirm their identity, but a request from a former staff member, or on behalf of someone else, would need to be verified using proof of identity, signature and address.

A parent / person with parental responsibility does not automatically have the right to make a SAR on behalf of their child, as the child has the right, and in all circumstances should be, considered in handling a SAR from a parent. A child of 13 or over will generally be considered able to consent to the SAR being made, or make a SAR on their own behalf, unless there are reasons to consider an older child cannot make that decision, or to consider a younger child able to make that decision. Also see the section on 'Content – Exemptions' under 'Responding to a SAR' below.

No charge: In most cases, a SAR will be responded to free of charge. In limited circumstances, where a request is manifestly unfounded or excessive an appropriate charge can be made. Requests made under EPIR 2005 may be charged for. A proposed charge should be agreed with the DPO.

Refusing to fulfil a SAR: In limited circumstances, the request or elements of it, may be refused:

- if the requestor cannot confirm their identity or authority to make the request on behalf of another person, the request will be refused until confirmation is provided;
- where a request is manifestly unfounded or excessive;
- information that might cause serious harm to the physical or mental health of the data subject or another individual;

Elements of the data held may be withheld or redacted, where:

- information that would reveal that a child is at risk of abuse, where disclosure of that information would not be in the child's best interests;
- information contained in adoption and parental order records;
- certain information given to a court in proceedings concerning a child.

A4.4 Responding to a SAR

Timescales: SARs must be responded to as soon as possible, and within **one month** at the latest. In the case of complex or multiple requests an extension of up to an extra two months can be applied, but the requestor must be informed of the extension within the first month from the SAR. The calculation of time will commence once the SAR is determined as valid. An acknowledgement should be sent to the requestor as soon as possible to inform them that the SAR has been received, the start date, and that it is being processed.

For SARs, school holidays, bank holidays and weekends are all **included** within the month. For example, a valid SAR received on 20th July should be fulfilled by 20th August despite the school closure.

Requests made under EPIR 2005 must be fulfilled within 15 **school days.**

Format: The DPO will decide with the requestor, the most appropriate and preferred method of providing information.

Content: The 'right to access' allows the requestor to receive information held about them, as a Data Subject. The requestor will not necessarily receive every version of information, if it is held in different ways or duplicated. Access is to the data, not the particular documents.

Third party data: Where the person's data is combined with another person's data, which does or could identify that other person (third party), that data may be redacted, or withheld if redaction would not fully prevent the other person being identified. Data can be disclosed that identifies the third party if, that person has given their consent to disclose it, or it is judged to be reasonable to disclose the information without that person's consent. Deciding if it is reasonable should take into account things such as the type of information, any duty of confidentiality owed, the role of the other person, whether the person is capable of giving consent, and whether they have expressly refused consent.

A4.5 Exemptions

Exemptions apply under the DPA 2018, allowing us to withhold data from a SAR in some circumstances, including amongst others: where legal professional privilege applies, where management forecasts or negotiations could be prejudiced by disclosing the data, confidential references, and where exam results are requested but they are not yet due to be published.

The application of exemptions should be approved by the DPO, but **if in doubt do not disclose information**, as it can always be disclosed at a later date.

Response: When sending the relevant data to the requestor, the information should be clear, so any codes or jargon used should be explained in the SAR response. In responding to requests we also explain to data subjects they have the right to make a complaint to the ICO or seek to enforce their rights through the courts.

Data subjects also have a right to receive, in response to their SAR, the following information, which is contained within our Privacy Notice (a copy of which will accompany the release):

- the purposes of our processing;
- the categories of personal data concerned;
- the recipients or categories of recipient we disclose the personal data to;
- retention periods for storing the personal data or, where this is not possible, our criteria for determining how long you will store it;
- the existence of their right to request rectification, erasure or restriction or to object to such processing;
- information about the source of the data, where it was not obtained directly from the individual;
- the existence of any automated decision-making (including profiling); and
- the safeguards we provide if we transfer their personal data to a third country or international organisation.

Monitoring: The receipt of SARs will be logged and coordinated centrally, using GDPRiS where appropriate, to ensure timescales are being met and SARs are being handled appropriately.

A4.6 SAR Request Form

Section 1

About yourself or person you are making this request on behalf of (Please use block capitals and black ink) – this information will help us to identify the personal data that we may hold about you.

Title (Mr /Mrs /Miss /Ms /Dr /Rev etc)	

Surname/Family Name	
First Name(s)	
Maiden/Former Name(s) (if applicable)	

Date of Birth (dd/mm/yyyy)	

Home Address (Include Postcode)	

This is the address to which all replies will be sent, unless you specify otherwise.

Name of person making request on behalf of data subject (if applicable)	
Surname/Family Name	
First Name(s)	
Relationship to data subject	
Preferred alternative address for correspondence (if applicable)	

Contact telephone number	
Contact e mail address	

Section 2- About your request

What records that you believe we hold would you like access to:

Have you made a request for this information before? (Yes/No)	
If Yes, could you please provide date of request? (dd/mm/yyyy)	

Where do you want to view your information? For example in person, or be sent a paper copy to your home or alternative address or be sent a copy in a specific electronic format to an e mail address (if this is your preferred option we would encrypt the file to keep it secure)
Do you need any other help with this request? (Please specify below)

Section 3 - Proof of identity

Establishing Proof of Identity

If we have a verified current address for you on our systems we will contact you at that address and ask you to confirm that the request has come from yourself.

If this is not possible, we will ask for documentary evidence to verify you are who you say you are.

To help establish your identity we may ask you to provide at least two different documents which, between them, provide sufficient information to prove your name, date of birth, current address and signature. For example, a combination of driving licence, medical card, birth/adoption certificate, passport and any other official documents e.g. utility bills, which show those details.

If you are making this request on behalf of someone else you must provide evidence you have the right to do so, e.g. letter of consent, birth certificate evidencing you have parental responsibility for a child or any other relevant legal documentation, unless you have supplied this information to us already for other purposes.

On receipt of completed form we will contact you to arrange verification of these documents.

Please note that it may be necessary to seek further information or proof of identity (of data subject or applicant) before the request can be processed. If this is the case, then the statutory one month day limit will start from the date all necessary information and proof is received. Every effort will be made to provide you

with your information as soon as possible after receipt of your application, however in some cases we may need longer than a month to respond to your request if any complex issues are involved.

Section 4 – Declaration

(To be signed by the Applicant)

The information, which I have supplied in this application, is correct, and I am the person to whom it relates/I have the right to make this request on their behalf *(delete as appropriate)*.

Signature	
Date	

Warning – A person who impersonates another or attempts to impersonate another may be guilty of an offence. It is similarly an offence to coerce consent from a Data Subject or interested third party.

Should any advice or guidance be required in completing this application, please contact our Data Protection Officer.

General advice on the GDPR and Data Protection Act 2018 can be obtained from The Information Commissioners' Office, contact details are below.

The information on this form will only be used to support you in exercising your rights under the Data Protection Act 2018 and will be destroyed, in line with our retention policy, after a decision on you request has been made. For further information on how Derbyshire County Council may use your personal information visit: www.derbyshire.gov.uk/privacynotices

Please return this form once completed to:

FAO Data Protection Officer at Repton Primary School

Mark your envelope "Subject Access Request - Confidential".

Data Protection Officer Name: GDPR for Schools, Derbyshire County Council

DPO Email: gdprforschools@derbyshire.gov.uk
DPO Phone: 01629 532888

DPO Address: Room 396, North Block, County Hall, Smedley Street, Matlock, Derbyshire, DE4 3AG

If however you are dissatisfied with our response, you can of course contact the ICO quoting our ICO registration number Z8588652 and stating that the Data Controller is Repton Primary School.

Information Commissioners' Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number
Fax: 01625 524 510. Website: https://ico.org.uk/concerns/

Annexe.5 Freedom of Information requests under the Freedom of Information Act 2000

A5.1 Introduction: what a publication scheme is and why it has been developed

One of the aims of the Freedom of Information Act 2000 (which is referred to as FOIA in the rest of this document) is that public authorities, including all maintained schools, should be clear and proactive about the information they will make public.

To do this we must produce a publication scheme, setting out:

- The classes of information which we publish or intend to publish;
- The manner in which the information will be published; and
- Whether the information is available free of charge or on payment.

The scheme covers information already published and information which is to be published in the future.

Most information in our publication scheme is available for you on our website. The remainder is available in paper form.

Some information which we hold may not be made public, for example personal information.

This publication scheme conforms to the model scheme for schools approved by the Information Commissioner.

A5.2 Values

At Repton Primary School we take pride in creating a vibrant school community based on equality, respect and inclusion. We develop inquisitive minds, as challenging questions and encourage deep answers. Our children have a real thirst for learning, becoming resilient and persevering when things get challenging. We pride ourselves in working closely with our community and all our families within it. Working together we have a shared responsibility to encourage aspirations and help all succeeded.

A5.3 Categories of information published

The publication scheme guides you to information which we currently publish (or have recently published) or which we will publish in the future. This is split into categories of information known as 'classes'. These are contained in section 6 of this scheme.

The classes of information that we undertake to make available are organised into 32 broad topic areas:

Governors' Documents – information published in governing body documents.
School Policies - information about policies that relate to pupils and the school curriculum and the school in general.

A5.4 How to request information

Where information is not published on our website, you may request a paper version of any of the documents within the scheme by contacting the school by telephone, email, or letter.

To help us process your request quickly, please clearly mark any correspondence **"FREEDOM OF INFORMATION ACT REQUEST**".

If the information you're looking for isn't available via the scheme and isn't on our website, you can still contact the school to ask if we have it

A5.5 Paying for information

Information published on our website is free, although you may incur costs from your Internet service provider. If you don't have Internet access, you can access our website using a local library or an Internet café.

Single copies of information covered by this publication are provided free unless stated otherwise in section 6. If however your request means that we have to do a lot of photocopying or printing, the following charges will apply:

- 5p per single side of A4,
- 10p per single side of A3.
- plus any postal charge at the current rate applied by Royal Mail.

For a priced item such as some printed publications or videos we will let you know the cost before fulfilling your request. Where there is a charge this will be indicated on application on an individual basis.

A5.6 Feedback and Complaints

If you want to make any comments about this publication scheme or if you require further assistance or wish to make a complaint please contact the School Office, Headteacher or School Data Protection Officer:

Data Protection Officer Name:	GDPR for Schools, Derbyshire County Council
DPO Email:	gdprforschools@derbyshire.gov.uk
DPO Phone:	01629 532888
DPO Address:	Room 396, North Block, County Hall, Smedley Street, Matlock, Derbyshire, DE4 3AG

If however you are dissatisfied with our response to your concerns you can of course contact the ICO quoting our ICO registration number Z8588652.

Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number
Fax: 01625 524 510
Website: https://ico.org.uk/concerns/