MILNROW PARISH CE PRIMARY SCHOOL

GDPR Policy

Document Control

Publication Date	25th May 2018
Related Legislation / Applicable Section of Legislation	Data Protection Act 2018 General Data Protection Regulation (GDPR) Digital Economy Act 2017 Human Rights Act 1998 Freedom of Information Act 2000 The Privacy and Electronic Communications Regulations EU e-Privacy Directive
Related Policies, Strategies, Guideline Documents	GDPR Privacy Notice
Replaces	Information Governance Policy
Policy Owner (Name/Position)	Milnrow Parish CE Primary School
Policy Author (Name/Position)	RMBC / Milnrow Parish CE Primary School

Review of Policy

Last Review Date	19th June 2018 revised 24.09.18
Review undertaken by	DPO
Next Review Date	This policy will be review following the enactment of the Data Protection Bill into law

Document Approvals

This document requires the following approvals.

Name	Title	Date of Approval	Version Number

Executive Summary

Information is a vital asset and resource, both in terms of the management of individuals and the efficient management of services and its support. It plays a key part in governance, service planning and performance management.

- Data Protection & Privacy
- Data Quality
- Information Security
- Information Sharing
- Records Management

Implementation of this policy will contribute significantly towards assuring the Schools stakeholders that information is being processed in compliance with legislation and School Policies. This policy will support the provision of high quality services by promoting the effective and appropriate use of information.

The governing body has overall responsibility for ensuring that the School complies with all relevant data protection obligations. The headteacher acts as the representative of the governing body on a day-to-day basis.

1. Introduction

The School is committed to protecting the privacy of individuals and handles all information in a manner that complies with relevant legislation & codes of practice including but not limited to the Data Protection Act 2018, General Data Protection Regulation, Digital Economy Act 2017, Human Rights Act 1998, Freedom of Information Act 2000 and common law duty of confidentiality. The School has established this policy to support that commitment.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record. Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

The Policy applies to all information held on paper or in electronic format including recorded information e.g. CCTV, voice recordings.

Everyone managing and handling information, particularly personal information, needs to understand their responsibilities in complying with the legislation & codes of practice. It is the personal responsibility of:

- All employees of the School
- All employees and agents of other organisations who directly or indirectly support or are procured by the School, including all temporary and agency staff directly or indirectly employed by the School
- Those engaged on interim contractual arrangements or agency contracts working on behalf of the School
- Suppliers and Data Processors of the School

The School recognises that there are risks associated with managing information in order to meet legislative and other requirements. This policy is intended to facilitate compliance & reduce risks regardless of how data is processed and all staff should be aware of its content and requirements. A number of guidance documents and information have been developed to support the application of this policy and the management of risk.

The School has a clear commitment to ensuring that all staff have access to appropriate training or guidance. Managers must ensure that those staff managing and handling personal & other information are adequately trained with regard to the requirements of this and all other Information Governance Policies.

The School will have processes in place to manage Induction, Refresher and Subject Area Training for all staff.

The School has implemented an awareness raising and communication process for Information Governance to keep staff up to date with new areas, policy updates and training requirements.

The School has arrangements in place to manage all legislative requirements including rocedures to manage requests made which as onown as 'individual rights' e.g. subject access requests.

The School has appointed the following roles to provide direction and oversight:

Data Protection Officer – is responsible for informing and advising the School of its obligations under data protection and privacy legislation and monitoring compliance. The DPO has a list of statutory tasks and has due regard to risk taking into account the nature, scope, context and purposes of processing.

If you need to **raise a concern** about our use of your personal information to our Data Protection Officer please contact DPOSchools@Rochdale.Gov.UK or Information Governance Unit, Number One Riverside, Smith Street, Rochdale OL16 1XU

2. Policy

2.1 Data Protection

The Data Protection Act 2018 and General Data Protection Regulation state how an organisation can use (process) personal information about individuals. The School has established this policy to ensure it meets legal requirements and has clear procedures and arrangements in place to manage compliance across all areas. Information will be processed lawfully, fairly and in a transparent manner in relation to the data subject.

The School is required to protect the rights and freedoms of individuals, in particular their right to protection of their personal data. This is not an absolute right and must be balanced against other fundamental rights and be considered alongside the principles of proportionality and necessity.

The School has a GDPR Privacy Notice in place. The GDPR Privacy Notice ensures that individuals are aware of how the School use their personal information. This is supported in other ways to tell customers how their information will be used e.g. verbally, forms and other corporate information such as leaflets. The School will use layered privacy notices, where necessary, to provide topic specific information where this is felt to be beneficial.

In order to operate efficiently, the School has to collect and use information about people with whom it works for a variety of different purposes depending upon the type of service it is providing. These are the specified, explicit and legitimate purposes referred to in legislation. These may include pupils and parents/guardians, members of the public, current, past and prospective employees and suppliers. The School will ensure that information is not further processed in a manner that is incompatible with those purposes and that the information collected is adequate, relevant and necessary for the purpose it is collected.

In addition, the school may be enabled required by law to collect and use information in order to carry out its functions as may be required by law and as directed by central government.

Whist the data that the School holds can be very useful in delivering & improving services, it also has a duty of care in respect of its handling and controlling access to this data especially in relation to personal, special category and criminal conviction and offence data.

The School will promote the use of Data Privacy Impact Assessments or similar arrangements to assist in identifying and minimising the privacy risks of new or existing projects, practices or policies.

The policy supports the rights of individuals to be informed of the risks and safeguards in place to

protect their information and how to exercise their rights in relation to that information. These include the right to be informed, right of access to data, right to portability and the right to object to processing.

It meets the requirements of the Protection of Freedoms Act 2012 in relation to processing biometric data.

2.2 Information Security

Information security is the practice of protecting information from unauthorised access or use, modification, accidental loss or destruction. The School has effective safeguards in place to make sure that personal and other information is kept securely and does not fall into the wrong hands. The School has clear procedures and arrangements to manage the human and technical elements of Information Security.

The School will maintain & protect all information assets both owned or used by the School to a high standard of confidentiality, integrity and availability. The School will ensure that information assets and hardware that are no longer needed are disposed of securely in line with industry standards.

Important information assets will include paper records stored on or off site, computers, mobile phones, emails, data files, software, recorded information e.g. CCTV, voice recordings.

The School will maintain an Information Asset Register to track, manage and dispose of these assets in line with legislative requirements & School Policy.

The School will ensure that any security incidents that occur are managed in line with current procedures for Information Security Breaches. It is the duty of all staff and other parties accessing or processing School data to immediately report any actual or suspected breaches in information security in line with School procedure.

Information Security Breach Procedure

Contents

1. Reporting Information Security Breaches

Milnrow Parish CE Primary School has implemented a consistent approach to dealing with all Information Security Breaches which must be maintained across the school. Potential Security Breaches must be reported immediately to the Data Controller, Headteacher, or in their absence the School Business Manager.

Centralised notification and control is necessary to ensure that immediate attention and appropriate resources are utilised to control, eliminate and determine the root cause of events that could:

- compromise data, specifically the personal or sensitive data relating to customers.
- disrupt the operation of the school or impact on other organisations and their networks.

Security Breaches have the potential to quickly escalate and spread across the organisation causing damage to equipment or data loss. All school staff must understand, and be able to identify Security Breaches and they must be reported immediately.

There are specific requirements to notify serious breaches to a variety of external bodies including the Information Commissioners Office who must be contacted in the first 72 hours on some

occasions. The School could be subject to an administrative fine from May 2018 if such breaches are not reported.

2. What is a Security Breach?

An information security breach would be caused when there is a failure to meet the requirements of the Data Protection Act or any compliance regime that the school is to.

- **Loss** of equipment
- **Loss** of data including paper records
- Unlawful **sharing** of personal data
- Sharing of **excessive** amounts of personal data
- A threat to the schools ICT Infrastructure

The School is required to manage & log actual breaches and **near misses**. For example:

An unencrypted laptop or Memory Stick containing personal data is lost or stolen	A fax containing sensitive information is sent to the wrong number
Paper records are lost or stolen (vehicle theft, burglary, left on the bus)	An email is sent with files attached containing personal data to the wrong email address (internally or externally)
Personal data is transferred electronically outside the workplace and is not encrypted or sent securely.	Personal data shared legitimately with a 3rd party is lost, stolen or used inappropriately.
Password Sharing	Breaches involving un-authorised access to the building
Paper records containing personal data are left unsecured (on a desk, at the printer)	A member of staff uses data for a personal rather than a work related reason – looking at a friends information.
Publication of technical code relating to the ICT Infrastructure	Comments posted on social media sites that breach confidentiality or identify an individual

3. Management of Information Security Breaches

ICT Security and Information Governance are viewed seriously by the school. Breaches may be under both the Schools Disciplinary Procedure and Information Security Breach Procedure or restricted to one of the two procedures. Dependent upon the seriousness of the allegations and outcome of investigations, which may lead to further action being taken against the school and employees should be aware that this may result in disciplinary action an outcome of which may have serious consequences for an employee's continued employment.

All breaches will be reported to the Data Controller, Headteacher for an initial assessment. A Security Breach Form and / or Incident Log **See Appendix B** may need to be completed for breaches and near misses.

Loss of equipment including mobile phones & laptops will be reported to the appropriate IT / Company to suspend any further use of this equipment. These are only classified as Security Breaches if they are not encrypted and there is personal or commercially sensitive information held on the device.

3.1 Process

The ICT breach management process will be followed incorporating 4 key steps – Initial Reporting, Managing the Breach, Investigating, and Final Report.

Day 1	•Notified to Data Controller, Headteacher with initial information
Day 3 (72 Hours)	•Advise from IG Unit where necessary •Decision on reporting to ICO •Agreed by Data Controller, Headteacher
15 - 20 Days	•Investigation Completed •Recommendations agreed by IG Unit and Headteacher,and plan for implementation developed

The breach will be logged on Information Security Breach Log.

Other resources may also be identified to support the investigation e.g. Security Manager or Building Manager. The investigation process will cover the following:

- Identification of the breach, analysis to ascertain its cause and any vulnerabilities it exploited
- Limiting or restricting further impact of the breach
- Tactics for containing the breach
- Corrective action to repair and prevent reoccurrence
- Consideration on informing the data subject of the breach

Once the investigation is completed, the Head Teacher/Chair of Governors will be notified that a breach has been investigated and a copy of the investigation report and recommendations will be included where necessary.

3.2 When might we have to report a breach?

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms which can include:

- potential negative consequences for individuals and adverse effects
- emotional distress
- physical and material damage.

If it's likely that there will be a risk then you must notify the ICO - this is referred to as a notifiable breach but should be a rare occurrence. If it's unlikely then you don't have to report it. The IG Unit will advise on this and documents the decision in the breach report.

When considering the requirement to report the breach to the ICO (within 72 hours), the time starts **when you become aware of the breach**. You do not have to have completed an investigation to report a breach; you can provide information at a later point.

When reporting a breach to the ICO, you must provide a description of the nature of the breach including:

- the categories and approximate number of individuals concerned
- the categories and approximate number of personal data records concerned
- the name and contact details of the data protection officer
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

This should be capture in the breach report.

3.3 Collection of Evidence

If a breach requires information to be collected for an investigation, strict rules must be adhered to.

The collection of evidence for a potential investigation must be approached with care and be carefully documented.

- The breach may need to be reported to the Information Commissioners Office (ICO) who will request a range of documents and evidence from the school
- There could be a complaint submitted to the school or though the Ombudsman
- There could be a further breach in the same area
- The school may need to consider disciplinary action following a security breach
- The basic details/statistics relating to security breach are becoming a popular FOI request

The following types of documents should be collated and included in the evidence folder:

Key Documents		
Initial notification of breach	Security Breach Form	Notification to Data Controller, Headteacher
Witness Statement (if required)	Emails to (where relevant)	Document index (where multiple documents have been lost/destroyed)
Training record for staff member - essential	Sign off by Headteacher	Communication across the school where agreed
ICO reporting Document (if required)	ICO Reference Number	Evidence of completion of actions
Evidence of procedural changes implemented following breach		

3.4 Risk Assessment

The breach should be risk assessed to determine the impact, particularly on individuals and whether they should be informed of the breach. This assessment includes the number of individuals affected, type of breach, potential reputational damage, media interest and potential litigation. There is a tool on the breach log to quantify this.

3.5 Learning from Information Security Breaches

Key components should be extracted from the Security Breach Form to learn from breaches, improve the response process and prioritise activities to improve compliance and reduce the recurrence of regular events. Any changes to the process made as a result of the Post Breach Review must be formally noted.

2.3 Data Quality

Consistent, high-quality, timely and comprehensive information is vital to support good decision-making, protect vulnerable people, improve outcomes for users & services and reduce unnecessary work. The School will ensure that information collected is accurate and, where necessary, kept up to date and will respond to requests from customers to correct the accuracy of their information.

Data quality is the responsibility of every member of staff collecting data or entering, extracting or analysing data from any of the School's information systems. All staff should know how their day-to-day job contributes information needed to deliver services and how lapses can affect, the School's reputation, financial penalties/fines, performance management, service delivery (particularly to vulnerable people) & the allocation of funding to the School.

2.4 Records Management

The School will ensure appropriate arrangements are in place for the care and management of its records to enable the school to meet its legal and regulatory requirements. School records will be accurate and accessible, giving a fair and truthful representation of the work and processes undertaken.

Effective records management is an integral part of achieving corporate goals and meeting legal and regulatory obligations. The School will manage records throughout their lifecycle from creation to eventual disposal thus ensuring that records are complete, authentic, trustworthy and secure and are available when needed. The School handles all records by following guidelines set out in P37 onwards in the IRMS Information Management Toolkit for Schools Version 5 which can be found following this link: https://c.ymcdn.com/sites/irms.site-ym.com/resource/collection/8BCEF755-0353-4F66-9877-CCDA4BFEEAC4/2016_IRMS_Toolkit_for_Schools_v5_Master.pdf
This outlines how long we retain certain types of information. We will only keep your personal information for as long as the law specifies or where the law does not specify this, for the length of time determined by our business requirements.

The School recognises that there are risks associated with managing records in order to meet the requirements of the Act. Non-compliance with this policy could have a significant effect on the efficient operation of the School and may result in financial loss and an inability to provide necessary services and information to customers. This policy is intended to mitigate those risks.

2.5 Information Sharing

The School will ensure that it is mindful of the legal basis for sharing data including personal data across its functions and with external partners especially in relation to non-routine data sharing or new projects where the sharing process changes in terms of purpose, parties, type of data, or means of sharing i.e. new computer systems etc. (the why, who what and how).
The School will ensure that in all cases where consent of an individual is required that the requisite privacy notices are given to individuals to enable them actively to give informed consent.

The School will use a range of Contractual terms, Data Processor and Information Sharing Agreements as may be appropriate to manage the sharing and disclosure of information to bodies within and outside the School.

Data Privacy Impact Assessments will be used, when required, at the outset for new projects, plans or policies that require the sharing of data to assess and mitigate risks identified and support good information sharing practice.

3. Monitoring Compliance and Effectiveness of the Policy Document

This policy will be subject to compliance audits instigated and overseen by the Data Protection Officer.

Information Governance is viewed seriously by the School. Any breach of this Policy and other associated requirements, will be considered and investigated under both the Schools Disciplinary Procedure and Information Security Breach Procedure or restricted to one of the two procedures. Dependent upon the seriousness of the allegations and outcome of investigations, and employees should be aware that this may result in disciplinary action an outcome of which may have serious consequences for an employee's continued employment.

If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s). Section 55 of the Data Protection Act 1998 makes it an offence to obtain, disclose or 'procure the disclosure' of confidential personal information 'knowingly or recklessly', without the consent of the organisation holding the data. Examples of a Section 55 offence include: misusing school systems to source information for personal use, 'hacking' of school systems, selling personal data held on a School system.

4. Policy Review Date

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed and updated when the Data Protection Bill becomes law (as the Data to capture any changes that will affect the Schools practice.

Appendix A – Data Protection Principles

Principle
5 (1)(a) processed lawfully, fairly and in a transparent manner in relation to the data subject
5 (1)(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
5 (1)(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
5 (1) (d) accurate and, where necessary, kept up to date
5 (1) (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
5 (1) (f) processed in a manner that ensures appropriate security of the personal data

Appendix B – Security Breach Form & Incident Log

Security Breach Form

The Information Asset Owner	
Data Controller	
ICO Registration Number	
ICO Registered Address	
Incident Case Reference :	

School Contact	
Name	
Job Title	
email address	
Telephone Number	
Postal Address	

Incident Date	
Report Date	
ICO Notification (Decision Date & Outcome)	
Investigating Officer	
Data Protection Officer Consulted	Yes/No
Investigation Completed	
Governors Notified	Yes/No

1. Details of Security Breach

A chronology - What happened? When (dates) did the actual breach/potential breach happen? When (dates) did you discover it had happened? How did you find out about the breach?

2. Findings

2.1 Types of Information and Number of Records

How many records were affected? e.g. 100 assessment reports, 1 email/letter
How many individuals were identified in the records or could be affected? e.g. 69 email recipients

2.2 Categories of data

Delete categories that do not apply

- Basic personal identifiers, e.g. name, contact details
- Criminal convictions, offences
- Data revealing racial or ethnic origin
- Economic and financial data, e.g. credit card numbers, bank details
- Gender reassignment data
- Genetic or biometric data
- Health data
- Identification data, e.g. usernames, passwords
- Location data
- Official documents, e.g. driving licences
- Political opinions

- Religious or philosophical beliefs
- Sex life data
- Sexual orientation data
- Trade union membership
- Not yet known
- Other (please give details below)

2.3 Categories of data subjects
Delete categories that do not apply

- Children
- Customers or prospective customers
- Employees
- Patients
- Students
- Subscribers
- Users
- Vulnerable adults e.g. identification of a specific characteristic
- Not yet known
- Other (please give details below)

2.4 What are the likely consequences of this breach on the individual(s)?
*Please describe the **possible** impact on data subjects, as a result of the breach. What areas have you considered? Please state if there has been any actual harm to data subjects*

2.5 What is the likelihood that data subjects will experience significant consequences as a result of the breach?
Delete categories that do not apply

- Very likely
- Likely
- Neutral – neither likely or unlikely
- Unlikely
- Very unlikely
- Not yet known

Please explain why you have come to this conclusion. What areas have you considered?

2.6 Have you told the data subject(s) of the breach?
Delete categories that do not apply

- Yes
- No, they're already aware
- No, but we are planning to / in the process of telling them
- No, we have decided not to
- We haven't decided yet
- Other

2.7 Risk Assessment of Current Practice
Describe the measures you had in place before the breach to prevent this happening e.g. staff training, policies, procedures or any other arrangements in place to protect this information.

2.7.1 Had the staff member(s) involved in this breach received data protection training in the last 2 years?
Staff member(s), date of training, method of training

3. Conclusion & Recommendations

3.1 Conclusion

3.2 Describe the actions you have taken or propose to take as a result of the breach to minimise to minimise the effect on individuals or change your practice in this area

3.3 Recommendations

Action	Who	Target Date	Completion Date

APPENDIX B Security Breach Form and Incident Log

Active	Reference	Type	Category	Brief Summa	Date Reported	Investigating/ Advising Officer	Signed off by	Sign Off Date	Summary to HR Date	Reported to ICO	Actions Completed	Action Lead	Actions Follow Up date
	Example	Incident	J Unauthorised	Email NOT bc	16/01/2017	XX	XXX		No	No	In Progress	XXX	15/04/2017
0	ISB.2018.001												
0	ISB.2018.002												
0	ISB.2018.003												
0	ISB.2018.004												
0	ISB.2018.005												
0	ISB.2018.006												
0	ISB.2018.007												
1	Current	Incident	A Corruption or inability to recover								In Progress		
0	Finalised	Near Miss	B Disclosed in Error								Completed		
		No Incident	C Lost In Transit								No Actions		
		Other Data (	D Lost or stolen										
		Draft Report	E Lost or stolen										
		Under Inves	F Non-secure										
			G Non-secure										
			H Uploaded to										
			I Technical security failing (including										
			J Unauthorised										
			K Other										

Appendix C – Glossary of Terms

Term	Meaning
Data Protection Act 1998	Historic legislation governing the protection of personal data and privacy in the UK.
Data Protection Act 2018	The main pieces of legislation that govern the protection of personal data and privacy in the UK.
General Data Protection Regulation	
Digital Economy Act 2017	Legislation allowing greater sharing and use of data across the public sector for purposes such as improving wellbeing and welfare, aiding research and combating fraud.
Human Rights Act 1998	Article 8 covers the right to respect for family, private life, home and correspondence and makes it unlawful for any public body to interfere with that right.
Data Privacy Impact Assessments	A tool to identify and address privacy risks for projects or changes in practice. Under GDPR, some DPIA need to be approved by the Information Commissioners Office.
Freedom of Information Act 2000	The main piece of legislation providing public access to (non-personal) information held by public authorities.
The Privacy and Electronic Communications Regulations	Sit alongside the Data Protection Act. They give people more privacy in relation to electronic communications.