CONFIDENTIAL

Data Protection Officer Audit (2019 Version)

Name Of School: Meadow View Primary School, Meadowhall Rd, Rotherham S61 2JD

Date: 15th January 2019

Review Conducted By: Tim Pinto

Staff Involved in the DPO Audit: Kerry Taylor (KT) – Business Manager

Introduction

The key principles of data protection under the Data Protection Act (2018) and the General Data Protection Regulation (2018) are that under Article 5(1) of the GDPR that personal data should be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals

b. collected for specified, explicit and legitimate purposes

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

d. accurate and, where necessary, kept up to date;

e. kept in a form which permits identification of data subjects for no longer than is necessary

f. processed in a manner that ensures appropriate security of the personal data

As a school, you have ' the controller shall be responsible for, and be able to demonstrate compliance'.

My role as your Data Protection Officer is to; 'assist you to monitor internal compliance, inform and advise on your data protection obligations'

The role of the audit is to ensure that your fulfil your obligations as a controller and processor.

Format Of The Report

The report will be series of questions (see below) which I will ask. If you are unable to answer them, they will be highlighted as 'UNANASWERED'. This will enable you to gather evidence as part of your action plan.

A short summary report will appear at the end with key areas to develop.

Policy/Document Review

This section is to ensure that the school has the policy structure in place to comply with the data protection principles.

Policy	Viewed	Comments
ICO Registration	Y	Registration Number: Z6700122. Expiry 20 May 2019.
Data Protection Policy	Y	The school has a Data Protection Policy which has been updated for GDPR/ Data Protection Act (2018). It is a very detailed document and highlights key areas such as subject access requests, retention and data security. It does need to include information about the role of the Data Protection Officer and highlight the relationship with the school.
Data Assets Inventory	Y	The school has audited its data assets in school and produced a list of paper and electronic data that it holds. It highlights where the data is kept and whether it is shared with a third party. It is a very detailed document and KT has been very meticulous in looking at what data the school holds. My recommendation is that there is a version control on the document, so changes can be tracked.

Data Sharing Agreements	Y	The school has begun to compile a list of data sharing agreements including the Local Authority and other organisations. It is a very comprehensive piece of work and KT has checked the privacy notices/GDPR statements from the third party processors. It is important that the if the school uses any company that directly captures data from parents and not via the school, then Meadowview needs to highlight that parents read the privacy notice for the third party processor.
School Privacy Notice	Y	The school has a privacy notice which has been developed in line with the Department of Education template. It is accessible and uses non technical language, so data subjects would find it easy to read. It is available on the school website. The school may want to include a statement that data follows the child through to secondary school and so Meadowview School may not retain specific information after Year 6.
Staff Privacy Notice	Y	The school has a privacy notice in place for staff. It is based on the Department of Education template and it covers the main aspects of data collection, sharing and rights of access that staff need to know. This document has not been issued to staff and it is important that it is emailed to all staff.
Acceptable Use Policy	Y	Pupil and staff have an AUP. It is important that additional statements are included on the staff AUP regarding accessing school emails on personal devices. This must include: • Staff must not use jailbroken phones. • All personal devices must have the latest software installed. • Only legitimate Apps must be installed on the device. • Devices must be set back to factory settings, if the device is sold. • All smartwatches must not be connected to mobile phones during school hours.
Privacy Impact Assessments	N	The school has not yet completed any PIA's. This is an area that needs to be addressed as the school needs to assess any high risk data actions. Examples of these can be when data is taken off site for school trips, when data is ported from different databases or when it is transferred to another school or organisation. A template is here: https://drive.google.com/file/d/1zgaRz3pf6p122VNvrpOn_r4B9YG9fBn8/view?usp=sharing

Admission/Capture Forms	Y	The school has an admission form for new starters. In line with data protection, they collate the correct amount of data and they are not excessive. The form does not include a statement around parent/carers asking permission for sharing emergency contact data with the school. The school completes a yearly data capture which is done via a blank form.
Freedom Of Information Policy	Y	At present, the school will use the RMBC model policy.
Roles	Y	KT is the business manager in school and this now includes data protection.
Data Transfer	Y	Procedure in place for transferring physical data. Other data is sent by recorded delivery.
Other	Y	The school has a number of other documents which include: • Retention Policy (Schedule) • Photography & Video Policy • Records Management Policy

Website

The section looks at what information it provides data subjects about processing and compliance regarding data collected from the school website.

Question	Y/N	Comments
Does the school have a Data Security section on its website?	Y	
Is it visible on the school home page?	Y	Under key information

Does it include the Data Protection Policy?	Y	
Does it include the Freedom of Information Policy?	N	
Is a privacy notice available on how the school processors data?	Y	
Does the school have a named Data Protection Officer with contact details?	N	
Does the site name the governor responsible for data security?	N	
Does the school offer guidance on how to make a subject access request?	Y	In Data Protection Policy
Does the school offer guidance on how to make complaints about the possible misuse of data?	N/A	This needs to be included in the DPP related to contacting the Data Protection Officer.
Is there a Code of Conduct available for the processing of children's data?	N	
Is a website policy available including privacy notice?	N	
Is there a Cookie Policy on the website?	N	
Does the school provide a translation tool for the above information?	N/A	
Does the school have an App? Has the school checked the privacy agreements with the software company?	N	

IT Infrastructure

The section will look at your provision for security (with your support of internal/external IT technicians)

This was completed by KT prior to the consultation.

IT Area	Y/N	Comment
Do you have an SLA with IT company?	Y	Impelling & RMBC (RGFL)
Does your SLA include actions by the IT company in relation to data breaches?	Y	GDPR policy sent as a separate document
Have you been advised with procedures to deal with ransomware/virus etc?	Y	1. The first stage is to isolate the computer from the internet and the internal network. In the case of ransomware we might need to perform a quick shutdown of the machine if it's performing any encryption. We'd then perform running tests in a lab environment, away from connection to the 'production' network and possibly back at Impelling base to prevent malware running when the computer is booted. 2) If the client cannot be fixed / cleaned then we'd perform a full wipe and restore from a non-infected backup. We would run a full system scan in school. 3) Finally we would aim to produce a report detailing what malware it was, where was the source (how did it get into the system) and what measure we should take to prevent future exploits.
Have you an AUP for staff/pupils?	Y	E safety policy
Do pupils have a password? Is it unique for username/password? Are there different actions between key stages?	N	Pupils use Year group logins (Year 1, Year 2 etc)

Do staff have complexity to their passwords?	Y	Must be 6 Characters long & contain characters from three of the following categories: Uppercase, lowercase, base 10 digits, non-alphanumeric characters and/or Unicode characters
Do staff have passwords for other systems e.g. SIMS	Y	Must be 6 Characters long & contain characters from three of the following categories: Uppercase, lowercase, base 10 digits, non-alphanumeric characters and/or Unicode characters
Does the school have 'guest' accounts for supply staff/trainee teachers etc.	Y	
Do staff have email disclaimers?	Y	
Do governors have a school-based email address?	Y	They all have an RGFL email account
Do you follow WEEE process?	Y	Old electrical equipment is collected by IT recycling companies
Are databases purged?	Y	Annually
Do you have an SLA with company that leases photocopiers?	Y	Xerox
Is the 'cache' wiped from photocopiers when it is taken off site?	Y	SBM to ensure this is done at the end of the lease.
Do staff have photocopier accounts which are password protected.	Y	Printings are held at printer until staff enter photocopier password
Do you have appropriate filtering in place?	Y	RGFL

Do you have anti-virus in place?	Y	Sophos
Have you a back up process in place?	Y	Encrypted device kept in the safe
Procedure for sending encrypted emails to outside agencies?	Yes	Via RGfL
Do you have security for where the servers are kept in schools? E.g. BIOS password, servers in cages?	Y	Servers are kept behind a locked door.

Data Offsite

This looks at your security measures for data that is taken offsite.

Question	Y/N	Comment
Do staff take any hardware offsite e.g. school laptops?	Y	Laptops which have double encryption
What security is in placed?	Y	Bitlocker Encryption
Are staff allowed to bring their own personal devices onsite?	N	Staff all have a laptop and ipads so do not need to use their own devices
Are staff allowed to access school based emails on their own personal device? Is there two factor authentication?	Y	Staff must login to emails via passwords not have them open on devices

Are staff allowed to use USB memory drives? School/Personal? Are they encrypted?	N	No school does not permit the use of pen drives in school.
Do staff ensure that data is 'signed off' when exchange documents at case conferences?	Y	We have in place a subject access request form which we get completed when information is shared with a 3rd party.

CCTV

Area	Y/N	Comment
Have you CCTV installed?	Y	
Do you use a third party company?	Y	Managed by ENGIE.
Have you defined your purposes for installing CCTV?	Y	
Have you carried out a Privacy Impact Assessment?	N	ENGIE need to supply a PIA.
Are images for their stated purpose e.g. crime prevention etc	Y	
Do you have a CCTV policy?	Y	
Do you review the system? 6 month/annually	Y	
Is it regularly maintained?	Y	

Is signage placed near cameras?	Y	
Do cameras view residential buildings?	N	
Are cameras external only?	N	A camera is in reception.
Do cameras view any private areas? E.g. toilets	N	
Provide name and address of school and a telephone number to contact about the camera.	N	There needs to be a sign in the front entrance, with the details of ENGIE as the company who maintain the CCTV system.
Ensure access to cameras and recorded images is restricted to authorized people only.	Y	Authorisation is decided by the headteacher.
Is the viewing of images restricted?	Y	The system is in the office and images are not viewable via the public window. On the occasions when recorded images have to be viewed, it is recommended that the entrance blind is pulled down.
Do you have security for the system?	Y	Kept in locked room.
Have you a retention period for CCTV images?	Y	28 days
Are CCTV images included in your Subject Access Requests?	Y	Release forms etc would be completed by ENGIE.

Site Visit

Areas viewed in the site visit are:

Areas	Security (Y/N)	Comments
Site Access – Does the school have a key management system?	Y	Fob system managed by ENGIE. KT responsible for key management system.
Site Access – does the school use keypad systems?	Y	The school does have keypad systems. The passcodes are changed as and when needed.
Office Area	Y	Locked room. Pupil data is kept in locked room adjoining the office. No personal/sensitive data is displayed.
Headteachers Office	Y	Keypad access to the room. There is an additional storeroom which holds personal/sensitive data and archived safeguarding data.
DSL Room	Y	Inclusion room (also incorporates SEND data). Locked filing cabinets. Keypad entry and no personal/sensitive data is displayed.
SEND Room	See above	See above
Classroom	Y	Data is kept in lockable cupboards.
Server Room	Y	Servers are kept in a locked room. Technicians have access to the room via key entry which is kept by KT.
Data Archive	Y	Room off office. Data retention management system in place.

Other	Y	Business Manager – Part of office area. Locked access. All personal/sensitive data is kept in locked filing cabinets Staff Room – Keypad access. No data displayed. Resource Room – Keypad access. Medical data is kept in locked cupboard. Kitchen – Allergy Data is displayed in kitchen area but it is not viewable.

Other Relevant Areas

The looks at other relevant data not included in earlier sections.

Area	Y/N	Comment
Does the school have a disposal procedure in place?	Y	An external company comes on site to destroy data. An invoice is kept by school. It is recommended that KT creates a data destruction spreadsheet recording what data has been destroyed.
Does the school have a procedure in place to deal with Subject Access Requests? What about six-week holidays?	Y	This is included in policies. The school also has a template for data subjects to complete. Emails are maintained over the summer holidays, however the school may want to look at including a statement on accessing post on the 'out of office' response during school holidays.
Do governors sign/view a privacy notice?	N	Governors have not been issued with a privacy notice. An example PN is here: https://bit.ly/2RiH1Ev
Do volunteers sign/view a privacy notice?	Y	Volunteers are issued with a privacy notice.

Do you have an exit strategy for staff?	Y	This is completed by KT and the school uses the HR portal. KT needs to ensure that all software accounts are deleted for any members of staff leaving, so they cannot access any data once they leave the school.
Do you seek permission for school photographs? • Website • Local Press • Social Media • Displays	Y	Meadowview has consent for images of children. The school uses Twitter, but do not share images of children.
What is the policy of taking photographs at school performances?	Y	Parents are allowed to take images of their child at the end of the performance.
Have staff had awareness training?	Y	Staff had training in the summer term (2018). It is regularly covered at staff meetings.
Is data protection part of new staff induction?	Y	New staff and students on placement receive data protection training.
Does the school check with third party contractors, that staff adhere to the data protection principles?	N	KT is to email RMBC regarding this.
Do you have a data breach procedure? Are all staff aware of the procedure?	Y	Yes, this is included in staff planners.
Do you have a process for children over 12 understanding their rights in the release of their data?	N/A	
Do you have an electronic visitor management system? Does it highlight where data is stored and how long it is retained?	N/A	The school uses paper books.
When pupils sign out, are parents able to view data about other subjects?	N	Parents now complete a slip, so they don't see any data from other data subjects.

Do you use biometric? If so, so you have a relevant policy?	N	
Do use you electronic communications with parents? If you use a third party, have parents signed a non-disclosure agreement?	Y	Text – Teachers to parents. Consent gained.
In your electronic communications with parents, do you use any form of direct marketing that falls within the Privacy and Electronic Communications Regulations (PECR)?	N/A	

Key Recommendations

- The school needs to begin completing Privacy Impact Assessments for any high risk data actions e.g. data transfer. A template can be downloaded here: https://drive.google.com/file/d/1zgaRz3pf6p122VNvrpOn_r4B9YG9fBn8/view?usp=sharing
- The staff AUP needs to be updated in order to include statements regarding staff accessing school based emails on personal devices.
- Governors at Meadowview school need to be issued with a privacy notice.
- As the school uses Twitter, it is recommended that they have a Twitter policy. An example from another school is here: http://www.gaerprimary.co.uk/files/Twitter%20Policy.pdf
- The school needs to contact the company that has created their website, about ensuring that it has a Cookies and Website (Privacy) Policy at the foot of its home page.