CONFIDENTIAL

Data Protection Officer Audit (April 2019 Version)

Name Of School: Saltersgate Junior School, Windsor Walk, Doncaster DN5 8NQ

Date: 10th June 2019

Review Conducted By: Tim Pinto

Staff Involved in the DPO Audit: Gillian Richardson (GR) – Business Manager, Paul Chambers (PC) - Headteacher

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 as ‘ 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 you 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 'Unanswered'. 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	The School is registered (ZA520257) on Tier 1. The expiry date is 16th June 2020. When the school re-registers, it may want to look at the following ,to see if it is registered on the correct tier: https://ico.org.uk/media/for-organisations/documents/2258205/dp-fee-guide-for-controllers-20180221.pdf
Data Protection Policy	Y	The school has a Data Protection Policy (DPP) which has been updated for GDPR/Data Protection Act 2018. It highlights the six key principles of collecting, processing and retaining data. It includes details of how data subjects can make requests which is accurate. It also includes the role of the Data Protection Officer and their relationship with the school.
Data Assets Inventory	Y	The school has audited its data assets and produced a directory of paper and electronic data that it holds. It highlights where the data is kept and whether it is shared with a third party. The spreadsheet

		template that GR is using is rather complex and I would look at adapting the DAI to a simpler format. Please see recommendations for further details.
Data Sharing Agreements	Y	GR has begun to collect a series of data sharing agreements from third party processors. This is important as the school needs to ensure that other companies/organisations are compliant with GDPR and adhere to the principles of legally storing pupil data. My recommendation is that the school has a single central register with all companies it shares data with e.g. school photographer etc and that this reviewed on a termly basis.
School Privacy Notice	Y	Saltersgate Juniors has a privacy notice which has been developed in line with the Department of Education template. It highlights the legal reasons for the collection, processing and the retention of data. It also explains the rights of data subjects in accessing and deleting data held by the school. It is available on the school website.
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. The school may also want to highlight the retention period for staff data in light of any SARS requests that are submitted by ex-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. It is also advised that the school have an IT loan form for the use of school-based hardware which staff use at home..

Privacy Impact Assessments	Y	Saltersgate Juniors has not yet completed any PIAs. 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.
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 school does not include a statement around parent/carers asking permission for sharing emergency contact data with the school. An example that could be included is: *As a parent/carer, I have sought permission from my emergency contacts to share their data with the school*.
Freedom Of Information Policy	Y	The school has a FOI policy which details the process of what data can be released and the process to do this. It is suggested that the school creates a publication scheme highlighting where data can be accessed. An example from another school is here: https://www.signhillsacademy.co.uk/_documents/%5B63084%5DFOI_Policy_Publication_Scheme.pdf
Roles	Y	GR and PC will deal with the 'day to day' issues relating to data protection. At present, there is no governor who has responsibility for data protection, however this will be addressed in the near future.
Data Transfer Procedure	Y	Proforma in place for the transfer of any physical data out of school.
Retention Schedule	Y	Protocol of record keeping which includes a full retention schedule, so GR knows when any data has to be destroyed.
Other Related Policies		IT Security Policy

Website

The section looks at what information the school provides for data subjects via the school website.

Question	Y/N	Comments
Does the school have a Data Protection section on its website?	Y	Under the 'About Us' section
Is it visible on the school home page?	Y	
Does it include the Data Protection Policy?	Y	This is in the 'Policies' section **NB This is an old policy and needs updating**
Does it include the Freedom of Information Policy?	Y	
Is a privacy notice available on how the school processes data about pupils/parents?	Y	Privacy Notice in the 'GDPR Section'
Does the school have a named Data Protection Officer with contact details?	Y	In the Privacy Notice
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	
Is a website policy available including privacy notice?	Y	
Is there a Cookie Policy on the website?	Y	
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/A	

IT Infrastructure

This section will look at how you ensure that all electronic data is kept securely in school and what measures are enforced to protect sensitive data when it is taken offsite.

IT Area	Y/N	Comment
Do you have a Service Level Agreement with an IT company?	Y	ACS
Does the school have a disaster recovery procedure in place e.g. additional electric backup for servers in the event of a power cut etc.		? *TP Comment – You need to ask ACS about an Uninterrupted Power Supply*.
Have you been advised with procedures to deal with ransomware/virus etc?	Y	
Have you an Acceptable Use Policy for staff/pupils?	Y	
Do pupils have a password? Is it unique for username/password? Are there different actions between key stages?	Y N	Pupils logon with the year they are from e.g. Year1, Year 2, Year 3
Do staff have complexity to their passwords? Is there enforced change? Do you have a different password	Y/N	Staff can set their own password. Not currently set to expire.

procedure in line with advice from the National Cyber Security Centre?		
Do staff have passwords for other systems e.g. SIMS. Does the school deploy any password manager software?	Y	No password manager software
Does the school have 'guest' accounts for supply staff/trainee teachers etc.	Y	
Do staff have email disclaimers?	N	
Do governors have a school-based email address?	N	
Do you follow the Waste Electrical and Electronic Equipment Directive (WEEE Directive) process?	Y	
Do you systematically review your electronic data stored on your servers to delete any old data in line with your retention policies?	Y	
Do you have an SLA with company that leases photocopiers?		*TP Comment – School did not answer*
Is the 'cache' wiped from photocopiers when it is taken off site?		*TP Comment – School did not answer*
Do staff have photocopier accounts which are password protected?	Y	
Do you have appropriate filtering in place?	Y	Sophos UTM (DMBC)

Do you have anti-virus in place?	Y	Sophos Antivirus
Have you a backup process in place?	Y	Backed up to NAS in locked server room
Procedure for sending encrypted emails to outside agencies?	Y	Feature on outlook
Do you have security for where the servers are kept in schools? E.g. BIOS password, servers in cages?	Y	Locked server room

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
What security is in place? Does this include any device management?	Y	Bit locker
Are staff allowed to bring their own personal devices onsite?	Y	Not connected to the internet
Are staff allowed to access school based emails on their own personal device? Is there two factor authentications?	Y	
Are staff allowed to use USB memory drives? School/Personal? Are they encrypted?	Y	

Do staff ensure that data is 'signed off' when exchange documents at case conferences?		*TP Comment – School did not answer*

CCTV

NB The school does not have a CCTV system.

Area	Y/N	Comment
Have you CCTV installed?		
Do you use a third party company which is able to monitor and view images?		
Have you defined your purposes for installing CCTV?		
Have you carried out a Privacy Impact Assessment?		
Are images for their stated purpose e.g. crime prevention etc		
Do you have a CCTV policy? **NB It is recommended that schools have a bespoke policy**		
Does your policy include a release form?		
Do you review the system? 6 month/annually		
Is it regularly maintained?		
Is signage placed near cameras?		
Do cameras view residential buildings?		

Are cameras external only?		
Do cameras view any private areas? E.g. toilets		
Provide name and address of school and a telephone number to contact about the camera.		
Ensure access to cameras and recorded images is restricted to authorized people only.		
Is the viewing of images restricted?		
Do you have security for the system? E.g. Is it in a locked room and/or cage?		
Have you a retention period for CCTV images?		
Are CCTV images included in your Subject Access Requests?		

Site Visit

This covers the physical security in place for room, filing cabinets and other areas on the school site that may include personal or sensitive data.

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 which is managed by a third-party company. Staff do not sign a fob lease form. The caretaker opens/locks school and is based onsite, so there is no need for additional keyholders. The school has a key safe and an informal key register.

Site Access – does the school use keypad systems?	Y	Access to playgrounds and front entrance. The passcode is changed when a member of staff leaves, or passcode compromised.
Office Area	Y	Fob access. Some data relating to evacuation plans for pupils displayed and PC will look at moving this, so it would not be viewed by those attending meetings in PC or GR's room. Medical data is displayed in the inside door of the main filing cabinet which is lockable.
Headteachers Office	Y	Restricted access. All appraisal data in locked filing cabinet. Some assessment data displayed; however, it is not highly sensitive data. It is advised that a cover sheet is put over this data when visitors are in the room. It is important that PC does not leave keys in filing cabinets.
Area that contains safeguarding data?	N/A	See office/headteachers room.
Area that contains SEND data?	Y	SENCO room. Cupboards which contain SEN data are in locked cupboards with restricted access. At the time of the audit, the room and cupboards were unlocked.
Classroom	N/A	Not visited.
Server Room	y	Kept in separate room off IT suite. The room is not locked, and it is advised that there is security in place when not used. There is ventilation in place.
Data Archive	y	In process of tidying up.
Staff Room	y	No data viewable in room.
Business Managers Room		Restricted area. Fob access. All HR data is kept in locked filing cabinets. No data displayed. Monitor has privacy screens.

Kitchen	Y	Allergy information is not viewable.
Other		

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	The school uses an external company (Shred It) to dispose of confidential waste. GR receives an invoice/certificate to ensure that this has been disposed securely. There are sealed confidential bins around school where sensitive data is placed. It is recommended that the school completes a model PIA for this action.
Does the school have a procedure in place to deal with Subject Access Requests? What about six-week holidays?	Y	Saltersgate Juniors has received no SAR over the past 12 months. The process of completing this is in the In the DPP which is available on the school website. GR is considering developing a template for data subjects to complete. There is some coverage of monitoring emails over the summer holidays, in the event of the school receiving a SAR.
Do governors sign/view a privacy notice?	N	Governors have not been issued with a privacy notice. It is important that they are issued with a PN, as this states how their data is processed and shared. An example of a governor privacy notice is available here: tiny.cc/598k8y
Do volunteers sign/view a privacy notice?	N/A	

Do you have an exit strategy for staff?	N	The school is developing a formal checklist for staff leaving the school that will cover all different accounts that they have access to e.g. CPOMS, SIMS etc.
Do you seek permission for school photographs? • Website • Local Press • Social Media • Displays	Y	Permission form that is sent to parents/carers. This covers all consents related to website, publications, social media etc. As the school uses Twitter, it is important that they have a specific Twitter account.
What is the policy of taking photographs at school performances?	Y	PC will make a decision at the start of performances related to whether parents are allowed to take photographs. This will be related to child protection issues.
Have staff had awareness training?	N	This will take place in September 2019.
Is data protection part of new staff induction?	N	This school will ensure that this occurs from September 2019 onwards.
Does the school check with third party contractors, that staff adhere to the data protection principles?	Y	A privacy notice has been given to some external contractors.
Do you have a data breach procedure? Are all staff aware of the procedure?	Y	There are procedures in place. Staff have PC contact details to inform him, if a data breach occurred during the school holiday period.
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?	Y	There is a statement next to the machine highlighting the processing of visitor data.

When pupils sign out, are parents able to view data about other subjects?	Y	Can see data from other students. This is a data risk, but the school will look at addressing this in future software updates of the electronic system.
Do you use biometric? If so, so you have a relevant policy?	N	
Do you use electronic communications with parents? If you use a third party, have parents signed a non-disclosure agreement?	N/A	Parents register using Parent Pay. It is important that parents understand that this is an external site and they should read the privacy notice related to the company who process their data.
In your electronic communications with parents, do you use any form of direct marketing that falls within the Privacy and Electronic Communications Regulations (PECR)?		

Key Recommendations

- It is strongly recommended that the school has agreement forms in place which are signed for by staff when fobs and school hardware are issued.

- It is important that staff lock filing cabinets which include sensitive data. Keys must not be left in any storage area that contains personal/sensitive data.

- The school needs to appoint a governor to oversee data protection and have a privacy notice in place for all governors.

- The school does have a Data Assets Inventory. However, it is recommended that it is simplified and includes the following areas:

    - Type of data

- What personal data is stored?
- How and why it is collected?
- Was consent obtained?
- Where is the data stored?
- Is it held by a third party?
- Does the school have a GDPR compliant contract?
- Security measures
- Who has access?
- Is it taken off site?
- Is it shared?
- How the school ensures the accuracy of documents?
- Retention period.

The DAI needs to cover the following personal/sensitive data: pupil data, HR (staff data), financial data, third party contractors, governor information, safeguarding, assessment, medical, appraisals etc.

-
- It is recommended that the school begins to complete privacy(data) impact assessments. These assess data risks for actions related to the use of information. Some examples are:

  - Sending sensitive information via recorded delivery (this can be a model PIA which is reviewed every year)
  - School trips or residentials where data is taken off site.
  - Laptops taken offsite by staff (model).
  - Using disposal company to destroy data(model)
  - Transferring pupil data electronically or by paper (model)