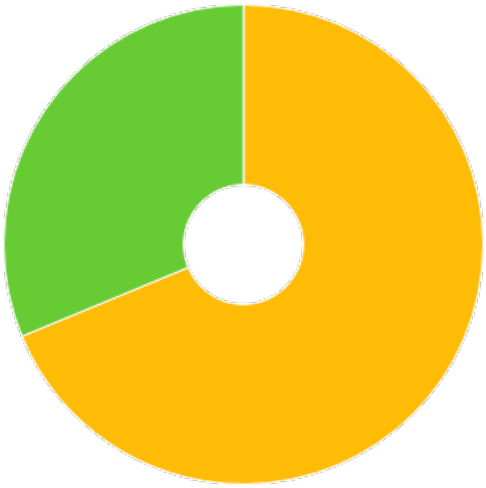
DPO Audit Report

School	Primrose Hill Primary School & Children's Centre
Reference	PB002796
Report date	21st March 2022
Auditor	Patrick Ballantine

Judicium have audited the data protection practices of the School on the date above. We have conducted our audit in line with data protection and freedom of information laws and best practice. The findings within this report can be shared with management to illustrate compliance and progression in following the required data protection legislation.

The recommendations made within this report have been provided to reflect the legal and best practice position as well as reflecting our responsibilities as the School's data protection officer. Ultimately the final decision in meeting the recommendations rests with management within the School. We will continue to follow up with you to monitor progress.

Summary of progression with GDPR



Key

Green
Currently meeting legal requirements and best practice of GDPR

Amber
Working towards meeting legal requirements and best practice of GDPR with actions required

Red
Not currently meeting legal requirements and best practice of GDPR

dataservices@judicium.com 020 7336 8403 72 Cannon Street London EC4N 6AE

Introduction and Summary

Key contact for data protection within the School
Lee Ashton - Headteacher

Is there a different contact during School closure periods
No

Date of audit
04-03-2022

Provisional date of next audit
06-03-2023

Overall summary of progress

Overall, Primrose Hill Primary School have achieved a pleasing level of compliance, with particular credit for the steps they are taking to make data protection a focus of the school's culture through regular meetings, briefings and training.

Going forward I advise that the school focus on ensuring that data maps are completed and all groups are provided with a privacy notice to better inform them how the school may use and share their data.

Should there be any concerns or queries with recommendations listed throughout this report, in theory or in practice, the school should not hesitate to contact Judicium Data Services for further support and guidance.

Registration and Awareness

Amber

What steps have been taken to raise awareness of data protection with staff? Please provide examples if necessary.
- GDPR meetings for staff,
- Privacy notice in place,
- Policy review on an annual basis,
- Bi-annual GDPR newsletters to reference best practice,
- School uses GDPR posters,
- Staff aware of the need to minimise data on display (ie newsletters) school has a radio channel to discuss data protection.
- High level of awareness, through information boards.
- Video training for new starters and on an annual basis for existing staff.
- Sign a self declaration form.

What steps have been taken to raise awareness of data protection with parents? Please provide examples if necessary.
- Privacy notice in place for parents and pupils,
- Parents receive briefings about data protection,
- Are invited to internet safety courses and briefings,
- The school anticipates being able to provide GDPR training to parents as part of NOS qualification.

What steps have been taken to raise awareness of data protection with children? Please provide examples if necessary.
N/A

What steps have been taken to raise awareness of data protection with governors? Please provide examples if necessary.
- Reminders on GDPR sent and informed on how the school is getting on with regard to data protection,
- Current privacy notice in place,
- Review policies and audit reports,
- Have not had formal data protection training as of yet.

ICO registration

- Registered
- Correct tier

Renewal date for ICO registration
08-10-2022

DPO details are within

- The website (under a data protection tab)
- Policies

Auditor's analysis

From the outset, the school has achieved a very high level of awareness. This has been accomplished through training and the regular provision and reviews or data protection, policies and reminders.

The school currently has included DPO details on the school website and current polices, however, will need to update current privacy notices and ICO registration to contain these contact details:

Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Lead Contact: Craig Stilwell

Recommendations

- Consider use of Judicium e-learning modules to build a curriculum for staff. (Due in 12 months)
- Provide data protection training for governors. (Due in 12 months)
- Add DPO details to ICO registration. (Due in 6 months)
- Add DPO details to Privacy Notices. (Due in 1 month)

Policies

Amber

The School have the following policies in place

Data protection policy

- In place
- On the website
- Accessible
- Includes subject access request procedure
- Staff aware

Data breach policy

- In place
- On the website
- Accessible
- Staff aware

Data retention policy

- In place
- On the website
- Staff aware
- Accessible

Freedom of information policy

- In place
- Up to date
- On the website
- Accessible
- Contains publication scheme
- Staff aware

IT / security policy(s)

- The school was unsure whether they had an IT security policy in place.

Are other data policies in place?
Acceptable Use Policies, Remote Learning Policies, Homeworking Policies.

How are cookies managed on the School website?

- Not in place
- School are creating a new website and have a policy in place for that.

Auditor's analysis

The school currently has all mandatory data protection policies in place, these are made easily accessible to internal and external parties and are regularly reviewed by staff. The only update to make to these policies is to update reference to current data protection legislation. Since Brexit, we no longer fall under (EU) GDPR but rather the UK GDPR. We are encouraging schools to make this change to account for deviations between the two which will more than likely appear in the future.

The school website does not currently have a cookie policy, however during audit I was made aware that the school will be migrating to use a new website shortly, when this is done the website will be required to have the following:

- a banner which alerts visitors to the use of cookies,
- this banner may also provide visitors the option to accept or decline these cookies,
- this banner should link to a cookie policy which will document what cookies are in use, and how they can be disable. A template version of this policy can be found through the Jedu portal under Documents/School Policies/Cookie Policy

Recommendations

- Draft and publish a cookie policy for the new school website, a template of this policy can be found through the Jedu portal. (Due in 1 month)
- Consider using an IT Security policy. (Due in 4 months)

Forms and Contracts

Amber

The School have the following contracts and forms in place

Contract of employment

- Contracts are issued by Salford.

Job application forms

- No privacy notice linked
- Up to date

Admissions/ pupil registration forms

- Privacy notice included within the pack
- Up to date

Recommendations

- Draft, publish and circulate a privacy notice for Job Applicants. A template of which can be found through the Jedu portal under Documents/Privacy Notices (Due in 1 month)

Data Protection Impact Assessments (DPIAs)

Amber

Have any new technologies been introduced since the last audit?
No

Please detail these new systems here.
N/A

Were DPIAs carried out before introducing these new systems?
N/A

Are DPIAs signed off by Judicium as DPO?
N/A

Are staff aware of the need to carry out DPIAs on new technologies/systems?
No

Auditor's analysis

The school has not adopted any new technologies since last audit and as such has not needed to complete a Data Protection Impact Assessment (DPIA).

Since the 25th of May 2018 it has been compulsory to complete a DPIA prior to processing data in a new way (i.e. sharing data with a new service). Completing a DPIA allows an organisation to fully understand the risk involved with processing data and to take action to mitigate any residual risk.

When the the school is next considering sharing or using data in a new way, they should contact Judicium Data Services for further guidance and assistance in completing this assessment.

Recommendations

- Conduct DPIAs for all new technologies, systems and services, informing Judicium Data Services when this is required. (Due in 12 months)

Privacy Notices

Amber

The School have the following privacy notices in place

Privacy notice for parents and pupils

- On the website
- In place
- Shared with new parents / pupils

Privacy notice for staff

- In place
- On the website / accessible
- In packs for new staff
- Shared with current staff

Privacy notice for job applicants

- The school does not currently have a privacy notice for job applicants.

Privacy notice for governors

- In place
- Shared

Privacy notice for visitors

- The school does not currently have a privacy notice for visitors.

Auditor's analysis

The school currently has privacy notices for parent, pupils governors, and staff. These notices will need to be updated to detail current DPO (Judicium) contact details as well as referencing current legislation (UK GDPR and the 2018 Data Protection Act).

Staff are required to review their privacy notice and are provided with a copy upon employment. Parents and pupils are also provided a copy upon admissions, however, steps could be taken to improve awareness surrounding the document. I advise that the school begin to routinely refer to this notice and where parents and pupils can find it. This could be done as a footer to regular parent communications, along the lines of: "Should you wish to learn more about data protection within the school, or review your privacy notice, please visit http://www.primrosehillprimary.co.uk/information/your-data/".

As the school processes the data of job applicants, and visitors, they will also need to draft and publish privacy notices for these groups and circulate them appropriately. I would always recommend that all privacy notices are included within the school website Your Data section. However the privacy notice for job applicants should also be included within job application documents, and a copy of the visitor privacy notice can also be held in the reception area of the school.

I would also advise that school refer to the Judicium template versions of these notices during this update and drafting process, these can be found through the Jedu portal under Documents/Privacy Notices. This will ensure that these notices have all the recommended provisions and sections.

Recommendations

- Alongside Judicium template versions, update privacy notices for staff, parents and pupils to reflect current legislation and DPO contact details. (Due in 1 month)
- Draft, publish and circulate privacy notices for job applicants, and visitors (Due in 1 month)
- Ensure to regularly refer to location of the parent and pupil privacy notice to ensure interested parties are fully aware of where to find and review this document. (Due in 4 months)

Data Requests

Amber

Have any subject access requests (SARs) or freedom of information requests (FOIs) been received since the date of the last audit?
No

Is there a policy in place detailing how to make requests?
This is detailed with the school's SAR and FOI policies.

If so, were they dealt with in accordance with legal timeframes?
N/A

Were any requests referred to the Information Commissioner's Office (ICO)?
N/A

Have requests been recorded on a data request log?
N/A

Recommendations

- Any future data request but be monitored and logged. The school should draft and publish a log for this, a template of which can be found through the Jedu portal under Documents/Logs and Registers. (Due in 12 months)

Training

Green

What data related training has taken place with staff?
Staff receive annual video based PowerPoint training.

Have records been kept of training
Yes

Do new staff receive training as part of induction?
Yes

Are there systems in place for refresher training for staff?
Yes

Auditor's analysis

The school have robust systems in place to ensure that all staff receive data protection training on an annual basis. They also build on this training through discussion during staff meetings to outline best practices.

To build and diversify their training offering, the school may also wish to consider use of some of Judicium' s e-learning training materials. These modules are school specific and can be allocated remotely. We have also developed a training matrix to help advise on which school groups should take which modules (this can be found under Documents/Training):

I would always advise encouraging staff to take the following core modules to ensure a wide foundation of knowledge:

- Introduction to GDPR and Data Protection
- What is a Breach
- Introduction to SAR and FoI Requests
- Breach Notification

Recommendations

Files

Green

What type of paper records are kept and how are they secured?

HR records

- Locked room
- Locked cabinet
- Limited access

Pupil records

- Locked cabinet
- Locked room
- Limited access

Safeguarding records

- Locked room
- Locked cabinet
- Limited access

SEN / ALN records

- Locked room
- Locked cabinet
- Limited access

Finance records

- Locked room
- Locked cabinet
- Limited access

What type of electronic records are kept and how are they secured?

HR records

- Password protected
- Limited access

Pupil records

- Password protected
- Limited access

Safeguarding records

- Password protected
- Limited access

SEN / ALN records

- Password protected
- Limited access

Finance records

- Password protected
- Limited access

Are access rights reviewed regularly to ensure appropriate access?
Yes

Is there a system in place for reviewing files to remove content no longer required (to comply with the principle of data minimisation)?
Yes

Auditor's analysis

There are excellent practices in place to secure and limit access to data and the school are aware that as staff roles change, access rights require review, this is done on an ad-hoc basis prompted by staff changes.

Recommendations

Emails

Amber

Who is the School's email provider?
Outlook via Salford

Have any of the following security settings been put in place for sending emails?

- Complex passwords to access email accounts
- Using secure portals which require a login to access the email
- Password protection on emails/attachments

Have retention procedures been put in place for emails?
School has an automatic deletion setting of 6 years, prior to deletion all emails are filed accordingly.

Auditor's analysis

The school has a retention procedure in place for staff emails, contents of emails inboxes are automatically deleted after 6 years. This is an excellent practices and vastly reduces the amount of data which the school may retain.

The school currently use password protection and secure online portals to share information externally. As all organisations are required to take all appropriate and proportionate means to protect data, I would advise that the school considers use of email encryption to protect data in transit. As the school uses Outlook, this can be enabled through the options settings, however the school may need to consult with their IT provided to assess how best this can be applied to all accounts.

Recommendations

- Consider use of email encryption for outgoing emails. (Due in 4 months)

Data Breaches and Reporting

Amber

What are the School's procedures for reporting a data breach?
This is documented in the school's data breach policy.

Have the School had any data breaches since the date of the last audit?
No

Have any breaches been referred to the ICO?
N/A

Do the School keep a data breach record?
N/A

Have staff have recent training/awareness on data breaches?
Yes

Recommendations

- In preparation for future data breaches, the school should draft a Data Breach Log in which they can be recorded. A template of which can be found through the Jedu portal under Documents/Logs and Registers (Due in 1 month)

Reasons for Processing

Amber

What steps are taken to ensure staff personal data is kept accurate and up to date?

- Complete contact sheets each year

When were the last reminders sent?
Reminders are not sent.

What steps are taken to ensure pupil/parent personal data is kept accurate and up to date?

- Self access to change own personal details

When were the last reminders sent?
Reminders are not sent.

Does the School gain consent for use of the following?

- Photos
- Social media
- Fundraising
- Marketing

How is personal data displayed throughout the School and are there safeguards in place?
The school ensure that displayed data is appropriately limited, to reduce the likelihood that it could be used to identify an individual.

Does the School have a record of processing activities or data map in place?
No

Auditor's analysis

The school keep the data which they receive up to date by providing parents with annual contact sheets and by providing staff with self access to keep their information up to date. To build on these best practices, I advise that the school begin to regularly remind staff and parents of the need to keep their information up to date, and for parents, how to inform the school of these changes.

Where data is displayed within the school, it is done for a distinct purpose and with appropriate security considerations.

The school should begin to develop a data map. This is a comprehensive document which lists all data that the school shares, who it is shared with and how it is then stored. Having one in place is an essential step for schools to improve on UK GDPR compliance. Once completed this map underlines the school's accountability to the data which they process as they have an easy reference for any current data sharing arrangement they have in place. This data map can be completed via the Jedu portal under the 'Data Mapping' tab.

Completing this map requires:
- the reason you are using the data,
- category of individual,
- categories of data processed,
- lawful use justification,
- types of recipients,
- whether this data is shared outside the EU,
- and where the data is located.

Once the information is inputted it will compile the map. Further instruction is provided within each section of the data map. For reference there is a data mapping key, guide and an example data map provided through the Jedu portal under Documents/Data Mapping.

Recommendations

- Issue regular reminders to parents and staff to keep their information up to date, and how they can do this. (Due in 12 months)
- Develop a data map or document which details types of data being processed, with who and on what grounds. (Due in 6 months)

Data Sharing with Third Parties

Green

Does the School have a data sharing register/record of third parties that they share data with?
Yes

If so, please detail this here.
Kept through GDPRis.

Are there contracts/privacy notices/data processing agreements in place with those third parties that cover data protection and security?
Yes

If so, please detail this here.
Kept through GDPRis.

Is there sufficient provision on sharing with third parties in the School's privacy notices?
Yes

Auditor's analysis

The school currently keeps a record of third parties to monitor their current data sharing arrangements, in addition to this they also collect data protection related documentation from third parties. This is an excellent practice and underlines the school's accountability for the data which they process.

Recommendations

Security

Amber

Who maintains the security network for the School?
IT Manager

How is security dealt with/monitored for building access?

- Perimeter fence
- Intercom / buzzer access to access past perimeter gates
- Intercom / buzzer access to reception
- Limited access to building
- Limited access to rooms within the building
- Visitors accompanied around or have lanyards

How is security dealt with/monitored for signing in?

- Use of electronic system
- Retention period for how long data is kept on system

How is security dealt with/monitored for system and network access?

- Each user has their own account
- Complex passwords required
- Automatically locked screens

How is security dealt with/monitored for back ups?
The school's databases and network is regularly backed up, these backups are appropriately secured.

How is security dealt with/monitored for printer and copier access?

- Use of pin coded/ follow me devices
- Regular checks of areas are done to ensure printing and copying isn't left lying around

How is security dealt with/monitored in classrooms?

- Sensitive data locked away
- Classrooms locked outside of working hours
- Automatically locked computers
- Regular checks of areas to ensure sensitive data is not left lying around

Auditor's analysis

There are excellent physical and security measures which have been taken to secure the school's physical and digital assets. In order to build on these best practices, I advise that the school consider implementing a Clear Desk policy. During audit we discussed that staff were aware of the need to clear away personal and sensitive data, however I would encourage committing this to a policy to evidence that this is being done. A draft version of this policy can be found through the Jedu portal under Documents/School Policies/Clear Desk Policy.

Recommendations

- Consider drafting and publishing a Clear Desk policy. (Due in 4 months)

Biometrics and CCTV

Green

Does the School use biometrics?

- No

If so, who uses it and where is it used?
N/A

Have the School gained the relevant consent for use of biometrics?

- N/A

What are the storage periods for retaining biometrics?
N/A

Have the School done a DPIA prior to its use?

- N/A

Does the School use CCTV?

- Yes

Where is it used?

- External areas
- Covers public areas
- Covers private property

How long/where is it stored?
Footage is kept for 7 days on an onsite server.

Who is the authorised person(s) for using CCTV?
Becky Cummins - Office Administrator

Do you have a policy on CCTV use?

- Yes

Is there appropriate signage on display?

- Yes

Can the CCTV do any of the following to help edit third parties from footage?

- None of the above

Have the School done a DPIA prior to its use?

- No
- CCTV has been in use since pre-GDPR.

Auditor's analysis

The school has excellent processes in place to regulate and control use and access to their CCTV. They have also clearly document its use within their CCTV policy. Should the current use of CCTV change, ie. new model of cameras, or new locations of cameras be used, the school should contact Judicium for advice and support.

Recommendations

Record Retention and Disposal

Amber

What does the School use for waste disposal (for personal data)?

- Shredders used on site
- Confidential waste provider who carries out waste disposal off-site

What security is in place to ensure disposal takes place correctly?

- Certificates of safe destruction provided by waste disposal company
- If taken off site, waste disposal company is a licensed waste carrier
- Security accreditation for waste disposal provider (such as ISO 27001)
- Confidential waste locked away
- Confidential waste in an area with limited access

Does the school use a data destruction log?
No

Auditor's analysis

The school securely archive data as it awaits destruction which is generally performed by a third party who dispose of data offsite. The school then received certificates of safe destruction from this third party.

The school are also required to document their large scale data destruction activities, as such they should use a Data Destruction Log to record these events and evidence the destruction of data. A template of this log can be found through the Jedu portal under Documents/Logs and Registers.

Recommendations

- Draft and publish a Data Destruction Log to record future large scale data destruction activities. (Due in 1 month)

Media Devices

Green

Hard Drives / USB Sticks

Are they used?

- Yes

Are staff allowed to bring their own hard drives/usb sticks into School to use?
No

What security measures are there in place for use of these devices?
These memory sticks are school issued and are encrypted.

Laptops/Macs/Ipads/Chromebooks/Tablets

Are they issued?

- Yes

Are staff allowed to take these devices home?
Yes

Are there any provisions in place to minimise risk to personal data when using these devices?

- Homeworking arrangements
- Password protection
- Two factor authentication
- Anti-virus and firewalls
- Encryption
- Pin protection

General

Do staff sign acceptable use agreements?
Yes

Does the School keep an asset register?
Yes

How are devices (and the data stored on them) disposed of when no longer needed?
By third party who destroy data and provide certificates.

Auditor's analysis

The school have ensured that all issued devices are appropriately secured and protected against unauthorised access, they also require staff to sign acceptable use agreements to ensure that they are aware of their responsibilities to the data which they may process when using these devices. Recognising that continued use of USB memory sticks pose a level of risk, the school have controlled this use by issuing encrypted devices for staff to use.

Recommendations

This concludes the audit report.

Our team are here to assist you with all aspects of compliance – please do contact us by email (dataservices@judicium.com) or by phone (0203 326 9174) if you have any questions or require any advice.

Our platform JEDU is a versatile resource which includes document templates, a data mapping tool and more!

You can access training for your staff through a separate platform designated for e-Learning courses designed by ourselves. You can log in at https://judiciumtraining.elearning247.com but if you have not registered yet, email us at the above address and we can help you get set up.