

DPO Audit Report



School Khalsa Primary School

Reference JS003639

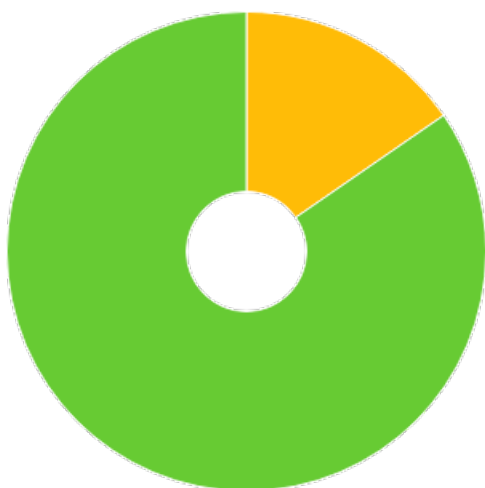
Report date 13th February 2023

Auditor Justyna Suldecka

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

Introduction and Summary

Date of audit

13-02-2023

Next audit date

February 2024

Are the list of school users up to date?

- Yes

Test

N/A

Summary of compliance

It was a pleasure meeting with Pat for the annual data protection audit.

There are a number of clear strengths for the school which include data protection awareness, signposting of data protection expectations through posters, up to date policies and good security procedures to keep personal data confidential and safe.

We have a couple of recommendations this year which include implementing a record of processing activities.

Overall, this has been another very strong year for Khalsa Primary School in data protection!

Registration

 Green

Are you correctly registered with the ICO?

- Yes

ICO registration number

ZA189200

ICO renewal date

26-06-2023

Are the DPO details documented on the ICO register of fee payers?

- Yes

Are the DPO details on the school's website?

- Detailed in policies

Auditor Comments

Registration is up to date.

Recommendations

Policies and Contracts

 Green

Data Protection Policy

- In place
- On the website
- Up to date
- Staff aware

Data Breach Policy

- In place
- Up to date
- Staff aware

Data Retention Policy

- In place
- Up to date
- Staff aware

Freedom of Information Policy

- In place
- Up to date
- Staff aware
- Contains publication scheme

Cookie Policy

- In place
- Up to date
- On the website
- Cookie pop up banner
- Option to accept/reject cookies

Employment Contracts

- Not yet updated

Auditor Comments

At the time of the audit, Pat presented a copy of the policies which are all up to date with the UK GDPR.

The policies are made available to staff internally in folders, as well as on the shared drive. Some of the policies are also available on the school website.

Employment contracts are provided through Ealing, so they refer to the 1998 Act rather than the updated version. All staff are given their own privacy notice with their contract. NB: Application forms through Ealing have been updated in line with UK GDPR.

Recommendations

Privacy Notices

 Green

Privacy Notice for Parents and Pupils

- In place
- Up to date
- Accessible
- Shared with new parents/pupils
- Shared with current parents/pupils

Has this notice been shared in the last twelve months?

- Yes

Privacy Notice for Staff

- In place
- Up to date
- Accessible
- Shared with new staff
- Shared with current staff

Has this notice been shared in the last twelve months?

- Yes

Privacy Notice for Job Applicants

- Application forms include a section on the Data Protection Act.
- In place
- Up to date
- Shared with job applicants

Privacy Notice for Governors

- In place
- Up to date
- Shared with new governors
- Shared with current governors

Has this notice been shared in the last twelve months?

- Yes

Privacy Notice for Visitors

- In place
- Up to date
- Shared with visitors

Auditor Comments

The Privacy Notices are all in place as detailed above. These are updated in line with Judicium's latest versions. Pat provided evidence of those during the audit and these were checked by consultant.

Pat ensures that individuals are reminded about their respective Privacy Notices.

Recommendations

CCTV and Biometrics

 Green

Is CCTV in place?

- Yes

CCTV Policy

- In place
- Up to date
- Accessible

CCTV Data

- Limited access
- Reasonable retention period
- Signs in place
- Footage is not in sensitive areas

Are biometrics in place?

- No

Biometrics policy

- N/A

Biometric data

- N/A

Auditor Comments

CCTV - up to date with a policy, retention is in line with requirements and no CCTV is placed in sensitive areas such as toilets.

Biometrics - not used.

Recommendations

Portable Media Devices

 Green

Which of the following devices do you issue to staff and students which can be taken off-site?

- Laptops
- Tablets

Are these devices encrypted and/or password protected?

- Yes

What security arrangements do you have in place for staff to securely access your network remotely?

- They are encrypted, staff have to access through TruSol if remote working and all staff are required to have complex passwords.

Which of the following arrangements are in place to protect the security of your school's devices?

- Asset register
- Acceptable use agreement
- Two factor authentication
- Home working arrangements

Are staff and students allowed to use their own devices to access school networks?

No.

Auditor Comments

Laptops and tablets are used at school. Laptops are taken off site, whereas tablets are used in-house only for presentations/photos. USBs are not used and Google Classrooms enable access remotely.

Asset register is in place and up to date, it is also checked by Ealing insurance department and this is signed by Chair of Governors.

Access review sheet is also completed with a checklist for leavers to give items back and this includes fobs to restrict access.

Recommendations

Data Security

 Green

What security policies do you have in place to protect data?

There are multiple policies for this including Information Security and Cyber Security Policy.

Do you have the following IT safety protocols to protect the data that you process?

- Firewalls
- Virus protection
- Staff awareness and/or training

Which of the following are done in relation to your back-ups?

- Carried out daily
- LGFL gridstone.

Are the following in place for cyber security?

- Complex passwords
- Regular software updates and patches enabled
- Staff awareness training

Auditor Comments

TruSol, IT consultants, complete checks on the system to ensure everything is up to date. Back-ups are frequently completed overnight and there are firewalls and antivirus in place to protect the network.

There are various security policies and this includes the Cyber Security Policy. There is good awareness around security at school and all staff are required to use complex passwords with a guidance note being sent out to them to explain this.

Recommendations

Training and Awareness

 Green

Has training been provided for governors?

- In progress

If so when was training last done and is there a record of it?

2019 through the eLearning platform. More recently, there have been sessions using PowerPoint slides which Pat presents.

Has training been provided for current staff?

- In progress

If so when was training last done and is there a record of it?

2019 through the eLearning platform. Pat uses PowerPoint slides to complete training.

Are there refreshers for all staff?

Yes. Annually.

Are there detailed training programmes in place for new starters?

- Yes

What awareness raising takes place with staff during the course of the year?

DPO Booklets are also utilised along with data protection information sent via emails.

Auditor Comments

Pat presents two PowerPoint slides and this is thorough. It is followed up with emails including information on complex passwords.

There are a number of posters around the school in areas where personal data is handled such as in the offices and reception area. Awareness raising takes place on an ad hoc basis and Pat ensures that everyone is aware of their data protection obligations.

Recommendations

Data Requests

 Green

Have there been any data requests since the last audit?

- Yes

If so, have they been dealt with in accordance with legal timeframes?

- Yes

Is your data request log up to date?

- Yes

Recommendations

Data Breaches

 Green

Have any data breaches occurred since the last audit?

- No

If so, were any reported to the ICO?

- N/A

Is your data breach log up to date?

- Yes

Recommendations

Data Principles in Practice

 Green

Do you have the following in place for consent?

- Consent forms in place
- Records of consent held
- Positive consent gained
- Consent forms up to date/regularly checked

Are regular reminders sent out to staff and parents to update their personal details?

- Yes

When were reminders last issued?

With staff this is completed once per year. School use Teacher2Parents to remind parents regularly.

Do you limit data kept on display within the school?

- Yes

How frequently do you conduct reviews/audits of personnel files to ensure only necessary data is kept?

- Annually

Auditor Comments

Consent is managed very carefully. This record is held on SIMS and the administrator can pull off a report from SIMS to check this and ensure that this is being followed. Data displayed is limited to what is necessary or to the information that individuals have consented to.

In line with the data accuracy principles, the school sends out notification to individuals to ensure their data is up to date on the school system. Files are also regularly reviewed for accuracy purposes.

Recommendations

Retention and Record Management

 Amber

Can you evidence how you follow retention procedures?

Data Retention Policy is followed.

Do ex-student and ex-staff records get archived when they have left the school?

- Yes
- Staff files are archived and the pupils' records are sent to the secondary setting.

Emails

Automatic on Outlook - 1 year.

Single Central Record

Leavers are moved to a leavers tab and these are held indefinitely. Recommended to keep in line with HR file which is 6 years after employment has ceased.

Signing in records

The InVentry system is reasonably new and these are held for up to 6 years.

Do you safely destroy physical records?

- Yes

Do you safely destroy electronic records?

- Yes

Is there a record of destruction for large scale files and records?

- Yes
- This was checked at the time of the audit.

Auditor Comments

Retention as a whole is very well managed with examples such as an email retention which is automatic on the system.

There is a destruction log in place and this is kept up to date.

We discussed that the leavers tab should be managed in line with the retention of HR files.

Recommendations

- To remove staff from leavers tab 6 years after they have left employment at Khalsa Primary School. (Due in 6 months)

Do you carry out DPIAs?

- Yes

Have your DPIAs been signed off by your DPO?

- Yes

Are the relevant staff aware of the need to complete DPIAs?

- Yes

What steps do you take to review your DPIAs?

School aware of this. No changes have been made.

Auditor Comments

DPIAs are completed for technologies that are higher risk in nature. There is an ongoing DPIA for Wonde which Judicium will assist with.

School are aware that DPIAs require a review when there are significant changes.

Recommendations**Information Sharing and Data Recording****Does your school have a record of processing activities or a data map in place?**

- In progress

When was this record last updated/reviewed?

This was not available to inspect at the time of the audit.

Do you transfer personal data outside of the UK/EU?

- No

Do you use any third parties who transfer personal data outside of the UK/EU?

- No

If you answered yes to either of the above two questions, do you have suitable agreements in place to safely transfer data outside of the UK/EU?

- N/A

What record do you keep of third parties that you share data with?

Yes. This is in a list format.

Auditor Comments

There is a data map in place but it was not available at the time of the audit.

We discussed that the Record of Processing Activities is a requirement and the school should finalise it and publish it on the school website.

The school do not transfer data outside of the EEA but are aware that should they wish to, they must contact us as the DPO so that we may advise.

There is a list of the third parties the school share personal data with and privacy notices/sharing agreements are retained in a folder for reference.

Recommendations

- To implement a Record of Processing Activities and to publish this on the school website. (Due in 2 months)