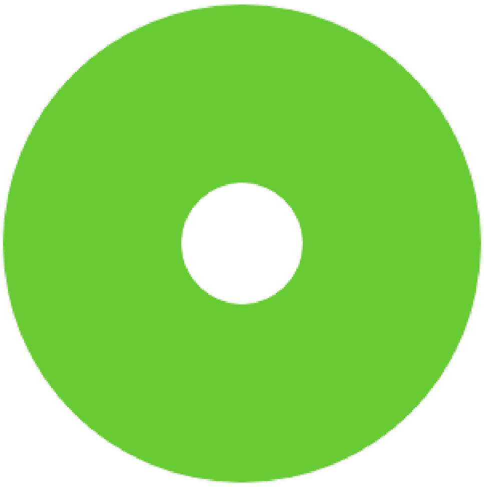
DPO Audit Report

School	Khalsa Primary School
Auditor	William Blanchard
Reference	WB001343
Report date	4th January 2021

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

Who is the key contact for data protection?
Pat Sheikh-Warak

Date of audit
17-11-2020

Provisional date of next audit
17-11-2021

Summary of compliance for management and governors

There is no denying that Khalsa and Pat have set a very high bench mark for data protection compliance in the work place. It is so deeply ingrained in to every working practice, that is now almost seamless.

Training amongst staff is excellent. All policies and privacy notices are up to date and regularly provided. The school makes sure that the data the collect to process on staff and pupils is accurate and up to date; this is reviewed at least once a year. Data and portable media devices are securely destroyed and Pat keeps a very thorough record of all of this. Finally, there are clear records of how data is processed, who it is shared with and for what reason. In all other areas Khalsa is excellent too.

In light of this I am very happy to say that I have recommended that Khalsa be awarded the Judicium certificate of excellence for data protection in the workplace to the Head of Department. Should he confirm this recommendation then you will be sent a digital certificate from our Team Administrator.

Part One: Follow Up From Last Audit

As a follow up to the last audit, we want to see how the school have progressed with the recommendations from the last report. Some of these recommendations may be repeated in sections two and three but we assess here overall how the school have worked on the outstanding recommendations.

The school won't need to have met all of the recommendations to be green, but we would expect about 70% to be completed.

How have you progressed in meeting the outstanding recommendations from the last report?
The only outstanding recommendation from the re-audit that WB undertook was to provide further training to staff, should Pat feel that staff required it. However, there is now a new training module that staff can take that is a refresher course to keep them up to speed on data protection at school, should Pat feel that it would be beneficial to staff.

Pat has given training to key staff who process data, and they have done the three core modules.

At the time of the last audit Khalsa VA Primary school were ranked as being excellent. It was clear that an enormous amount of time, effort and hard work had been put in by Pat to ensure that all policies and procedures were up to date, and oftentimes, they were what we would advocate as best practice.

Part Two: Compliance - ICO Registration

● Green

Section 2 is the compliance section. This is checking day to day compliance with data protection laws and principles. There is a mixture of legal requirement and best practice built within our analysis and recommendations. Where it is best practice we do try to make this clear and this doesn't always change the compliance colour if it's not deemed a necessary change.

Have you registered with the ICO?
Yes

Has the date for renewal expired or is it upcoming?
It is now up on the system and the expiry data is 26 June 2021 (ZA189200).

Are Judicium's details on the ICO registration (as DPO)
No

Are you Tier 1 or Tier 2 registered?
Tier 1

Recommendations

- To add Judicium as your DPO to the ICO register. (Due in 3 months)

Governors

● Green

Have governors received training?
Data protection discuss data protection during meetings. Pat discusses it with them. They have a privacy notice. Overall, the governors are well versed in data protection matters at Khalsa Primary School.

Do you have a privacy notice for governors?
Yes

Has the privacy notice been shared with governors?
Yes

Are audit reports shared with governors?
Yes, they are shared by the governors.

Are data policies approved by governors?
Yes

Auditor's Analysis

Governors have an active role in data protection at Khalsa. Whilst they have not received formal training by undertaking the Governors' e-learning module they have received training from Pat in governor meetings, and it is a topic that is regularly discussed. There is a privacy notice for governors which is shared with then at least once a year and they are all involved in the ratification of relevant data protection documents.

Recommendations

- To consider providing the e-learning training to the governing body. (Due in 6 months)

Staff

● Green

Have staff received training in the last two years?
Admin staff have all received training in the form of a presentation and the three core modules. The main body of staff have regular GDPR updates and key training points that they need to be aware of.

Do new staff receive training?
They are updated on arrival and are then given regular updates.

Is there an up to date privacy notice for staff?
Yes

Have staff received a copy of the staff privacy notice?
Yes

When was the privacy notice last issued/reminded to staff?
In the last couple of months.

Is the privacy notice on the website?
Yes, this is clearly on the website alongside a multitude of other privacy notices.

How are privacy notices issued to new staff?
They are made available on the website to all staff.

Is the employment contract up to date?
Yes, the employment contract is up to date.

Is the employment application form up to date?
Yes and there is a privacy notice for job applicants made available on the school's website.

Are reminders sent to staff to ensure their contact details are up to date?
Once a year, but they do this routinely throughout the year.

What do staff do to keep personal data out of display in their rooms/offices?
Clean desk policy, lock classroom, don't leave any data out - Pat sent out an email at the start of October 2020 to ensure that all staff are aware of this.

Are all staff required to have complex passwords to access the network?
Yes, all staff are required to have complex password.

Auditor's Analysis

All staff have received formal training and get regular updates in staff meetings and briefings. There is a specific staff privacy notice which is shared at least once a year, provided to new starters before they begin and is readily available on the website.

Contracts and forms have all been updated to make sure they reflect the current legislation

Recommendations

Pupils and Parents

● Green

Is there an up to date privacy notice for pupils and parents?
Yes

Have parents received a copy of the privacy notice?
Yes

When was the privacy notice last issued/reminded to parents?
It was sent out at the start of the this academic year.

Is the privacy notice on the website?
Yes, it is available on the website.

Are the consent forms for use of images up to date?
Yes, and they are all made available on the website.

Are admissions forms up to date?
Yes, they are up to date.

Are reminders sent to parents to ensure their contact details are up to date?
Once a year but parents are always very good at ensuring that their data is kept up to date. Reminders are put in the weekly newsletters.

Auditor's Analysis

Again this is another area where the school are very strong. The privacy notice is on the website for parents to find. It is provided to parents at least annually and Pat makes sure to collect parents' data to keep it as accurate and up to date as possible.

Recommendations

Policies

🟢 Green

Do you have the following?

- Data protection policy
- Subject access request policy/appendix
- Data retention policy
- Data breach policy
- IT safety / security policies
- Freedom of information policy and publication scheme
- Social Media Policy; Clear Desk Policy; Photograph Consent Form for Governors and Volunteers and another for Staff; GDPR Addendum to Ealing Employment Contracts; GDPR Privacy Notice for School Governors and Volunteers; GDPR Privacy Notice to Staff; GDPR Privacy Notice to Parents; GDPR Privacy Notice for Visitors and Contractors; and GDPR Privacy Notice for Job Applications.
- CCTV policy

Are these all up to date?
Yes, these are all up to date.

Are the policies accessible?
Yes, they have all been made available on the school's website.

Do policies have a review date ?
Yes, every policy has a date confirming when it was last reviewed and when it is expected to be reviewed by.

Is there a notice and policy on the website for cookies?
Yes, there is notice on the website for cookies.

Auditor's Analysis

All the policies are in place. They have all been made available on the website. Pat has additionally curated other policies that are beneficial to both students and staff at Khalsa. There is a cookie notice and banner on the website.

Overall, this is again, very good.

Recommendations

Data Requests

● Green

Do you have a data request log?
Yes.

Have data requests been made since the last audit?
Yes, three data requests. One SAR and two FoI requests.

Were they answered in accordance with timeframes?
Yes.

Did requests get referred to the ICO?
No.

Auditor's Analysis

All data requests were handled in accordance with the legislative timelines, all this information has been recorded on the school's data request log which I confirmed during the audit.

Recommendations

Data Breaches

● Green

Is there a breach log in place?
Yes.

Have any breaches been reported since the last audit?
No.

Were any breaches reported to the ICO?
N/A

Auditor's Analysis

Whilst no data breaches have taken place, there is a data breach log prepared in case one occurs. All staff have received training on what to do in case of a data breach.

Recommendations

Data Protection Impact Assessments (DPIA)

● Green

Have you carried out any DPIAs since the date of the last audit?
Just one.

If so, were these DPIAs signed off by Judicium?
Yes, it was signed off.

Have DPIAs been reviewed for progress?
Yes, Pat keeps an eye on them.

Recommendations

- To contact Judicium when next undertaking a DPIA as we have an extensive library of templates at your disposal. (Due in 9 months)

Data Mapping and Sharing

● Green

Do you have a data map or record of processing activities?
Yes there is an up to date record of processing activities.

Is there a data sharing register?
Yes, this is up to date as well.

Do you hold (or know the location of) third party contracts and notices which cover data protection obligations?
Yes, Pat has all the privacy notices in a file and has recorded them in the record of processing activities.

Recommendations

CCTV

● Green

Is CCTV used?
Yes

Does it monitor public or sensitive spaces?
No it does not.

How long is CCTV kept for?
Thirty days.

Is there a responsible user for CCTV?
Yes, it's Pat and the site manager.

Recommendations

Part Three: Retention

● Green

We are placing a lot of focus on data retention in this audit. Good retention practice can help:

- Ensure good safeguarding/SEN practice
- Avoid complaints or issues from staff/pupils/parents
- Protect others by keeping accurate records
- Decrease the risk of a data breach
- Help save time in future in dealing with data requests
- Free up space (both physical and digital space)

However we are aware that there are other factors to consider (such as lack of time and budget cuts). But our guidance is designed to be fluid to factor in these points. We do encourage schools to try and place some time into retention structure as this can help save time in the future (for example by making data requests easier to respond to, or meaning file reviews will be done quicker).

Who is responsible for data retention and destruction management?
Pat is responsible for data retention.

Do you have different levels of access to paper records?
Yes, only certain members of staff are allowed to view certain information.

Do you have different levels of access to electronic records
User access privilege,

Do staff have their own drives?
Yes

What is done to maintain those drives?
Staff share one drive which TruSol ensure that there is nothing kept in there for any longer than required.

Auditor's Analysis

Data is appropriately managed as outlined above. Access to electronic and the limited paper records is reviewed regularly and the School, ensure that access is tiered for both processes.

All sensitive data is limited to only authorised staff members to ensure that security is adopted carefully.

Recommendations

Key Records

🟢 Green

Personnel

Are personnel files managed regularly?
Yes, they are managed regularly.

Do files appear organised?
Yes, they are all organised.

Are retention periods followed for personnel files?
Yes, Pat has a very comprehensive file documenting when documents should be destroyed after their relevant archive period.

Pupil

How long are pupil files kept for?
They are passed whole sale on to secondary school.

Does the school retain SEN and safeguarding records separately?
Yes, these are kept separately.

Safeguarding

How long are safeguarding records kept for?
Some records are retained in accordance with the school's legal requirements and everything else is passed on to the next school.

How are safeguarding files secured?
Locked in a cabinet, keys are in the HT's room.

Electronic Records

What large-scale electronic records are stored?
SIMS, 3BM, SCR.

What retention periods are followed for those electronic records?
All retention periods are recorded in the retention folder and Pat ensures they are all followed.

How long are the following records retained for: -

Finance records
Six years.

Biometric records
N/A.

Pupil work books
These are sent home with pupils.

Signing in records
Six years.

Auditor's Analysis

Data retention as highlighted above is managed very well by the School as a whole.

The School has an up to date Data Retention Policy which is followed appropriately. Pat has a very detailed system set up to confirm when data should be destroyed and once it has been destroyed this is marked off on the school's data destruction log.

Recommendations

Single Central Record

● Green

Do you have a single central record?
Yes.

Does it contain the necessary detail?
Yes it contains all the necessary detail.

Does the record include agency staff, contractors and volunteers?
Yes, it includes all of those.

Is it up to date?
Yes.

Auditor's Analysis

The Single Central Record is accurate and up to date in line with the Ofsted and legislative requirements .

Recommendations

Emails

● Green

Is there a retention procedure for emails?
Yes, the school uses the LGfL retention period.

How is this enforced?
This is enforced by LGfL

Do those users who send emails externally have tighter security on their accounts?
Staff have access to Egress.

Auditor's Analysis

The School has the capacity to send secure and encrypted emails. All staff are versed on how to do this should they wish to send any personal data outside of the School. though this is usually limited to very small number of people who would be involved in this.

There is a retention period in place for emails through LGfL, which the School uses to ensure that no superfluous emails are retained.

Recommendations

Asset Register

● Green

Do you have an asset register?
Yes, there is an asset register.

Does it contain necessary detail?
Yes.

Is it up to date?
Yes.

Auditor's Analysis

The asset register is accurate, up to date and regularly reviewed.

Recommendations

Devices

🟢 Green

USB Sticks / Hard Drives

Are they issued?
No

Are staff allowed to use their own?
No

If they are used are they encrypted?

Remote Working

Do staff use remote working?
Staff can use their school laptops. TruSol provide a link to staff to ensure that everything is secure. There is currently only one tablet, but the school will be buying another.

Laptops

Are they issued?
Yes

Are they taken off-site?
Yes

Are they encrypted?
Yes

Are staff required to have a complex password to log on?
Yes

Do you have acceptable use agreements in place for their use?
Yes

IPads

Are they issued?
Yes

Are they taken off-site?
No

Are staff required to have a pin/password to access the tablet?
Yes

Do you have acceptable use agreements in place for their use?
Yes

Auditor's Analysis

No USB sticks are allowed to be used by staff. Instead they are provided with laptops that they can take off site to work from. Access is granted securely by TruSol. All portable media devices are encrypted and password protected.

Security has really been thought about and put at the forefront here.

There is additionally an acceptable use agreement that all staff have to sign before being able to use any portable media devices.

Recommendations

Data Destruction

● Green

What do you use for destruction of paper?
All shredding is done in-house.

For confidential waste, do you shred on site or off site?
On-site shredding.

For electronic devices, how are they disposed of?
A third party comes in wipes the hard drive, give Pat the certificate and then they would dispose of the laptop.

How are USB sticks disposed of?
N/A.

How are laptops and ipads disposed of?
A third party comes in wipes the hard drive, give Pat the certificate and then they would dispose of the laptop.

Do you use a waste destruction log?
Pat has a folder in which she records when specific data should be destroyed in line with the Khalsa retention policy and once that data has been destroyed it is marked off as such.

Auditor's Analysis

All destruction of data is done on site and is over seen by Pat. This is done securely through shredding and is done all year round.

Portable media devices, when they become obsolete, are taken off site, wipe clean and recycled. Pat has all the destruction certificates from these.

Overall, this is another area where the School is strong.

Recommendations