In Support of Learning

Warwickshire Education Services

SCHOOL DATA PROTECTION OFFICER

Longwill School for Deaf Children

(part of the Birmingham Special Schools Trust)

School DPO Service GDPR Compliance Audit 2020-2021

Purpose of Audit

As part of your subscription to the School DPO Service we carried out an audit within your school /academy trust in line with the UK GDPR and to ensure you are complying with data protection legislation.

Scope of the audit

To complete this audit, we have requested documentation to verify that your school has implemented measures that demonstrate compliance with data protection legislation. We also interviewed key members of staff to get an understanding of their level of knowledge regarding data protection and how compliance works in practice. We have reviewed all of the information collected both from your documentation and staff interviews and have recorded our findings within this report.

For each area we have reviewed we have provided a rating. Where you have scored a rating of Amber or Red, we have provided you with recommendations. Please be aware that we are on hand to support you with this and if you require any further guidance on implementing those recommendations, please do not hesitate to contact us.

Green	The school demonstrates a high assurance of data protection compliance
Amber	Areas have been identified for improvement.
Red	Little or no evidence to demonstrate compliance.

Section 1– Outcome of Audit Meeting

Overall, your school demonstrates compliance with data protection laws and is taking steps to ensure good practice. The school has appointed a team to lead on data protection matters who share a good level of knowledge of the requirements of data protection laws.

The school has produced the recommended and mandatory policies as they have now implemented a comprehensive information security policy. The school have also implemented procedures that demonstrate a high assurance of data protection compliance.

Where we identified from our discussions any areas where the school could go further to demonstrate best practice, we provided an action point in the summary of discussion document. We have also listed them below for ease of reference.

As discussed during the audit meeting, we recommend the school review their current processes to ensure they can demonstrate effective information risk management. This would include gaining a deeper understanding of data protection impact assessments and adopting a process that allows the school to consider DPIAs as part of their project proposals. I have enclosed a DPIA flow chart, which the school may utilise as part of their current processes. There is further information on DPIAs within Bulletin 14 and the school may also find the exemplar DPIA contained within Bulletin 22 to be of some use in the event they were to carry out an assessment. The School DPO Service are also working on a further Bulletin on DPIAs, which we hope to be available later in the summer term.

Action points highlighted during our discussions:

- The data protection/ GDPR Privacy team are planning to have monthly meetings to discuss data protection matters and review and update documentation as appropriate.
- We will review the school's consent documentation; however, it is important to ensure these documents inform individuals of their right to withdraw their consent. This can be achieved by adding the statement below.

  'Please note, you have the right to withdraw or change your consent at any time by giving the school written notice and completing a new consent form. You can notify us of your consent withdrawal in writing by contacting {insert relevant school email address}.'

- Consider the recommendation from the DfE, for schools to review their data protection policy annually. The school are currently working on centralising staff data protection training.
- Consider implementing the enclosed subject access request process and log. This will allow for effective management and recording of such requests should the school receive any.

- Consider implementing the enclosed DPIA flow chart into the school's process when considering any new project proposals.
- The school are working on finalising their information security policy. We have enclosed a word version of our exemplar policy to assist with this process.

We have completed a review of your school's documentation and used the outcome of this review, along with information provided during the audit meeting, to complete the rest of the school's audit report. You will note our recommendations within each of the relevant sections.

Section 2 - Document Review

Data Mapping Tool

Article 30 of the UK GDPR requires organisations to keep records of their data processing activities, sometimes referred to as ROPA or a data mapping exercise. These records should be granular in detail and ensure they capture the following details: -

- Categories of data subject (e.g. parent, pupil, staff, visitors or governors)
- Your lawful reasons for processing (this will include reasons for the collecting of data as well as the lawful reason for sharing the data).
- The categories of data (e.g. identify which data is special category data)
- Details of third-party receivers of the data (all third parties with whom you regularly share the data)
- Relevant safeguards (e.g., identify the risks and the measures in place to mitigate those risks)
- Links to relevant polices/details of retention/security measures (please note that we are still working on building this into the exemplar data map).

Overall, the school has detailed records of their data processing activities. However, we have made the following observations:

- Currently, the school's data map groups data together to record the overall record rather than specific sets of data. E.g., 'Pupil Records'. We recommend granulising these records to set out what data would be processed within these records. E.g., name, contact details, date of birth etc. This will allow the school to accurately identify their lawful reasons for processing. Your lawful reasons for processing a pupil's name may be different to the reasons in which you process their contact details. This is particular relevant when detailing who you share that data with.
- Where you have identified 'Legal Obligation' to process the data, you should be able to identify the piece of legislation that obliges the school to collect and process this data. It would therefore be useful to have this information recorded in your data mapping exercise.
- Your data map does not currently record from where the school has obtained the data or detail any third parties with whom you regular share the data. It is important to document how the data flows into the school, what happens to it whilst you hold the information, and

where the data goes when shared externally. You will then need to identify your lawful reasons for sharing the information.

The school may wish to refer to our exemplar data mapping tool contained within Bulletin 19 when reviewing the above recommendations.

Overall Rating **AMBER**

Data Collection and Consent

The school have provided us with their data collection form, which is appropriately written and does not request any information that would be deemed unnecessary. This form also directs individuals to the school's privacy notice for details on how their data will be used.

We also reviewed the consent form for images. This consent form is appropriately written and contains the necessary elements required to meet the standards of valid consent. However, as discussed during our audit meeting, the form does not advise individuals of their right to amend or withdraw their consent choices or how they would be able to exercise this right. We therefore recommend that you add the following wording to your school's consent documentation.

Please note, you have the right to withdraw or change your consent at any time by giving the school written notice and completing a new consent form. You can notify us of your consent withdrawal in writing by contacting {insert relevant school email address}.

Overall Rating **AMBER**

Data Protection Policy

The school has implemented a comprehensive data protection policy, which sets out how the school will comply with data protection legislation. This policy has been appropriately shared with staff and is published in a suitable location on the school's website.

As discussed during the audit meeting, the DfE recommend that this policy is reviewed annually.

Overall Rating **GREEN**

ICO Registration

The school is currently registered on Tier 2 with the Information Commissioner's Office. However, as the school is a foundation special school and holds a charitable status, the guidance from the ICO suggests that the school would be entitled to register on Tier 1. This would incur a lower fee.

The school are in touch with the ICO to establish the correct Tier and will update their registration details if appropriate.

Overall Rating **GREEN**

Data Protection Champion

The school has appointed a team to lead on data protection matters who all demonstrate a good knowledge of data protection laws.

The team are setting up regular meetings to review the school's status of data protection compliance, review documentation to ensure it is accurate and up to date, to establish an effective process to ensure a culture of awareness, and that compliance is monitored throughout the year.

Overall Rating **GREEN**

Privacy Notices

The school has produced privacy notices for, pupils, staff, and governors.

The school's privacy notices are accurate and detailed in their content.

We recommend the school amend their pupil privacy notice to also reference the data that is processed in relation to parents. This can be achieved by referring to parents in the document title and reviewing the content to ensure data relating to parents is included in the notice.

We also recommend adding data tables to your notices that would provide further details on how and why data is processed. The privacy notice data tables are our recommended means of communicating how the school uses information in a clear and transparent manner. This is not a specific requirement of data protection legislation; however, schools should ensure that individuals are fully informed on how and why you are processing their data.

Overall, the school's privacy notice provides the required information to your data subjects. The school review the information detailed in the privacy notice in line with the information contained in the school's data map.

Overall Rating **GREEN**
(with minor recommendation)

Data Breaches

The school has an effective process for responding to, recording, and reporting data breaches.

This process is contained in the school's data protection policy which has been shared with staff.

The school's data breach log is detailed and thorough and demonstrates that the school's data breach process is working effectively.

Overall Rating **GREEN**

Subject Access Requests

The school have not yet received any subject access requests, but they have a log in place to record any requests they do receive.

The school also addresses Subject Access Requests within the Data Protection Policy and advise individuals of their data rights within their Privacy Notices. At the time of the audit meeting, the school did not have a documented process for responding to SARs and we have therefore provided a process map. We recommended the school review this process in the event they were to receive a request.

Overall Rating **GREEN**

Information Security Policy

During our audit meeting, the school were working on their Information Security Policy. However, we noted the school to have various policies that would address information security and that in practice, information is managed in a secure manner. The school have adopted a culture of clear desks and ensure staff have secure storage for both manual and electronic information.

At the time of writing this report, we observed the school to have since implemented a stand-alone Information Security Policy, which is published on the school's website. This is a comprehensive policy that clearly sets out how the school will keep information secure.

Overall Rating **GREEN**

Data Sharing

During our audit meeting, the school confirmed they keep a record of all third parties with whom they regularly share data. However, these records would need to be reviewed following various updates to legislation.

We also asked about data protection compliant agreements with third party processors. Again, this is something the school are aware of and believe the relevant agreements are in place and that these need to be reviewed in line with updated legislation.

We have not reviewed any evidence of the school's data sharing records and have therefore not provided a specific rating for this area. The school may wish to review the general guidance detailed below and utilise the resources with Bulletin 21 when they carry out their review of their data sharing records.

Data sharing guidance in brief:

Schools should ensure they operate due diligence when sharing information with third parties and should be aware of the requirements of the UK GDPR to ensure the appropriate assurances and safeguards are in place.

Article 28 of the UK GDPR requires all organisations to have a written agreement with all third-party data processors. The clauses to be included in that agreement are also outlined in legislation so it is important to ensure these agreements are reviewed to check they are GDPR compliant.

The UK GDPR also makes it illegal to share data with other countries who are not covered by the GDPR or included in the list of 'approved' countries, without the adequate safeguards in place. It is therefore imperative to know where the third-party store their data or where their servers are located.

This is complex area of data protection compliance and we recommend you seek advice from the DPO Service when looking to sign up to any new third-party processor. However, you should ensure you have fully reviewed any current third-party processors to ensure you are complying with your legal obligations.

We recommend all schools carryout the following steps to ensure they can demonstrate their compliance with data protection laws:

- Compile a list of all third-party processors (this will be a third party who processes data on the school's behalf and in accordance with your instructions).

- Review the documentation you have in place with each third party to ensure it meets the requirements of Article 28 of the UK GDPR – The School DPO Service will happily assist with this.

- In the absence of any documentation, or if you cannot locate a copy of any agreements in place; contact the third-party Data Protection Officer to request a copy of the 'agreement required under Article 28 of the GDPR'. Alternatively, issue the third party with a Data Processing Agreement (an exemplar can be found in Bulletin 21).

- Record all steps taken and any assurances you have in place, within your Data Sharing Log - again, an exemplar log can be found in Bulletin 21.

There is no legal requirement to have such agreements with third-party Data Controllers. This will be third parties where you will have no control over how that data is processed. Examples would include the local authority, DfE, NHS. However, it is important to still carryout due diligence before sharing the data. If possible, we would recommend you look to adopt a data sharing agreement with such third parties. An exemplar Data Sharing Agreement can be found in Bulletin 21.

Information Risk Management

During our audit meeting, we discussed effective information risk management and how this is demonstrated through the consideration and completion of data protection impact assessments (DPIAs). The School's data protection leads have some knowledge of DPIAs but are yet to complete an assessment. We advised the school to review the resources available from the DPO Service, both in Bulletin 14 and the documents provided following our meeting, to establish a process that demonstrates the consideration of information risk management as part of any project or plan.

A DPIA is a 'risk assessment' process designed to help you analyse, identify, and minimise the data protection risks of existing or proposed processing of personal data. Carrying out a DPIA is mandatory for some data processing activities, so it is important to be familiar with the process of conducting a DPIA and being able to 'screen' the data processing activity to establish whether a DPIA would be required.

A DPIA should be conducted where the processing is 'likely to result in high risk to the rights and freedoms of natural persons'.

It is mandatory for a DPIA to be conducted in the following circumstances:

- Systematic monitoring of publicly accessible places on a large scale e.g. CCTV
- Processing of special category data or criminal offence data on a large scale e.g. processing of biometric data or high volume of safeguarding information.
- Systematic and extensive automated processing that leads to decisions with significant effects regarding individuals e.g. profiling individuals

You should ensure you keep accurate records of your DPIAs and ensure that the outcomes of your DPIAs are integrated into your projects. A DPIA is not a one of exercise and you should ensure you have a process to ensure they are regularly reviewed.

It is important to note that the school do not carry out any processing that would automatically mandate the need for a DPIA. However, it is important for key members of staff to have an understanding of Data Protection Impact Assessments and for the school to implement a process to ensure staff consider these assessments as part of any project or plan.

Following our audit meeting, we provided the school with a flow chart that would act as a documented process for screening for DPIAs. We also recommended the school review the information and resources contained within Bulletin 14.

The School DPO Service have an exemplar CCTV DPIA within Bulletin 14, an exemplar DPIA for remote learning within Bulletin 22, and an exemplar DPIA for sharing information in connection with COVID-19. We also have exemplars for processing data in relation to safeguarding information and processing biometric data for cashless catering systems. Please get in touch with the DPO Service if you require copies of any of these exemplars.

Should you need any assistance with completing a DPIA, please get in touch with us and we will do our best to assist.

Overall Rating **AMBER**

Training and awareness

The school have provided training records, which detail the data protection training and safeguarding training undertaken by staff. Although there is reference to key members of staff having received training, there was no reference to all staff having received data protection training. However, we noted during our audit meeting that the data protection leads were working to centralise the staff data protection training records. We have therefore based your rating on the evidence we have been presented with.

During the audit meeting, we also noted the school were considering how they could incorporate data protection training as part of the induction process.

We recommend all staff receive data protection training and that this is regularly refreshed. If all staff have not yet received data protection training, there are resources available from the School DPO Service that are accessible to schools as part of their subscription. This includes access for all staff to an eLearning training platform, a training video that can be watched individually or as a group during inset days, PowerPoint slides, and various webinars for data protection leads.

In light of the above, we recommend the following:

- Review their current training records and ensure all staff have received data protection training and that these records are centralised.
- Should any member of staff have not received data protection training, or in the event training is due to be refreshed, consider the resources available from the DPO Service.
- Record any informal training to demonstrate how the school ensure a culture of awareness, e.g., reminders, updates, staff briefings, emails, handouts etc.

If the school would like to utilise any of the training resources available from the School DPO Service, please do not hesitate to get in touch with us.

Overall Rating **AMBER**

Records management

The school operate to retention schedules set by the local authority. Archives are securely stored on school site and the school ensure they have secure storage for any electronic files.

We discussed the approach to managing the records the school retain and whether archives are regularly reviewed to ensure retention schedules are being adhered to. There has been

lots of work already carried out by the school to achieve effective records management and although this is still a work in progress, it is acknowledged that the school have made great progress with this.

The school will find resources within Bulletin 20, which may prove to be useful when establishing an effective process to managing information.

We would have no further recommendations for the school at this time, other than to continue to work on the archiving held by the school to ensure they are not retaining information for longer than necessary.

Overall Rating **GREEN**

Conclusion

You will note our recommendations within the individual sections of this report. Please look to action these as soon as you are able to do so. We have provided links below to the Bulletins you may find of use when reviewing these areas.

Please remember that the School DPO Service are on hand to provide support and guidance wherever we can so please get in touch with us if you need any further assistance. Our contact details are listed below for your information.

School DPO Service
Warwickshire Legal Services
Warwickshire County Council
Shire Hall
Warwick
CV34 4RL
Direct 01926 412859
schoolDPO@warwickshire.gov.uk

Bulletin links

Bulletin 1 – Welcome

Bulletin 2 – Data Mapping Tool

Bulletin 3 – Consent/ ICO registration

Bulletin 4 – Lawful basis for processing

Bulletin 5 – Information Security

Bulletin 6 – Privacy Notice

Bulletin 7 – Introducing DPO Team

Bulletin 8 – Contracts/Privacy Notice Tables

Bulletin 8.5 – Data sharing – Contracts/Variation Schedule

Bulletin 9 – Data Protection Policy/Governors and Applicant Privacy Notice

Bulletin 10 – Data Sharing/Processing Agreement

Bulletin 11 – Data Breaches

Bulletin 12 – Subject Access Requests

Bulletin 13 – E-learning materials

Bulletin 14 – DPIAs

Bulletin 15 – Corrections & FAQs

Bulletin 16 – Data Processing & Data Sharing Agreements & Subject Access Requests

Bulletin 17 – Data Tables for Staff and Governors

Bulletin 18 – FAQs

Bulletin 19 – Data Mapping Tool

Bulletin 20 - Retention

Bulletin 21 – Data Sharing

Bulletin 22 – GDPR and Remote Education, Update on International Data Transfers & Meet your DPO Team

Bulletin 23 - DPO Service Update (Audit Process for 2020/21 & E-Learning Training)) (NB: Link for the E-Learning Training form doesn't work in bulletin - this is the link DPO E-Learning access request (Hutsix))

Bulletin 24 - Lateral Flow Testing and Updates (05/02/21)

Training Materials #1 - Being an Effective DPL (26/03/21 - contains Annual Checklist, template training log, and recording of webinar)

Training Materials #2 – Handling Data Breaches (28/04/21 - contains slides, procedure, and recording of webinar)

Training Materials #3 – Dealing with Data Rights (09/06/21 - contains slides and tale of data rights)

Training Materials #4 – Information Security (14/07/21 - contains slides)

Update to schools - September 2021 training video and audit process