What to Expect from our Data Protection Health Check/Review

This document explains our approach to your health check, what you need to do and the timescales. The aim of the health check is to determine and assess the School's level of compliance with the main requirements of the European General Data Protection Regulation (GDPR) and the Data Protection Act 2018. If your School carries out digital direct marketing, then we will also assess its compliance with the relevant provisions of the Privacy and Electronic (EC) Communications Regulations 2003 (PECR).

There are 5 distinct steps to the health check and your help is needed at each stage:

Step 1 - Information Gathering

We agree a mutually convenient date for us to visit you in School to interview key staff. The visit will last 1 day.

When you have booked your health check, we ask you to send us key School documents. For example, Data Protection Policies, Privacy Notices etc. We review these before we visit you to help give us an early indication of how your school approaches data protection.

We also send you 6 interview questionnaires in advance to give you the time and opportunity to gather in the information required to answer the questions. If you are at all unsure about a question, you can contact us for help. It is preferable to require the relevant key colleagues to answer the questions that relate to the areas they manage. For example, questions relating to admissions should be answered by your Admissions team, questions about IT should be completed by your IT lead and questions about fundraising and development completed by your Development team etc. However, it is reasonable for the School's data protection lead to be involved with this and to help them answer the questions.

This step in the process will involve significant effort on the School's part and we recommend you take at least 4 weeks to do it. However, in gathering together this information, you will become more familiar with the processing undertaken and be better prepared for the actual interview.

We will need you to return the key documents and the draft completed questionnaires to us no later than 3 weeks before our visit. Any delay in sending us these documents will likely result in the health check interviews being rearranged.

Step 2 – Preparing for the Staff Interview

We will review your draft completed questionnaires and key School documentation.

Step 3 - Staff Interview/our Visit

The staff interview is the most critical part of the Health Check because we use the output to measure what is happening in practice.

The interview takes place with the data protection lead plus one other member of staff such as your IT lead. To avoid wasting your IT lead's time, he or she can join the interview at the point in time when we are asking IT questions. We can agree this with you in advance. *It is not possible with a health check to interview more staff than this.* Those interviewed will be speaking on behalf of the colleagues that completed the draft questionnaires.

All interviews must take place within a 'working day' i.e. 10.00am - 5.00pm with a 45-minute break at lunch.

In most cases, it is perfectly possible to conduct your interview/s remotely by telephone or Skype. Please discuss this with us in advance if this is your preference or if bad weather prevents us getting to you.

Step 4 - Report Writing

After the interview we will review all of the information gathered and write your Compliance Report. The Compliance Report is initially provided in draft form to the school data protection lead for their comment. This allows us to modify and amend where required.

We aim to provide your draft report within 8 weeks of having conducted the staff interview. In most cases, it will be with you sooner than this. If there is any outstanding information which we have requested (For example, because of matters becoming evident during interviews) but have not received, this may result in a delay in the draft report being produced.

Your report will comprise the following material:

- A guide to navigating the report
- An Executive Summary of the School's position including an overview of remedial measures recommended. This is ideal to share with Governors and other senior leaders who will need to understand the outcome and risks at a high level but without all the detail.
- A table of recommended actions. (We use the traffic light system so you can see at a glance which actions are the most urgent.)
- Appendices relating to each main area of the health check. These contain all of the detail underpinning our recommendations and are ideal for reference purposes and for those that need to know more.
- Useful information and links.

Step 5 – Production of the Final Report

If any amendments to the report are required i.e. in light of comments made on the first draft, we will update the report and provide the responsible member of staff with a final draft within an agreed time frame.

The ISBA/iLP Data Protection Health Check

Frequently Asked Questions

What is the aim of the health check?

The aim of the health check is to determine and assess the School's level of compliance with the main requirements of the European General Data Protection Regulation (GDPR) as they apply to the UK and the Data Protection Act 2018. If your School carries out digital direct marketing, then we will also assess its compliance with the relevant provisions of the Privacy and Electronic (EC) Communications Regulations 2003 (PECR).

Who created the health check?

Our health check is the result of a joint project between The Independent Schools' Bursars Association (ISBA) and The Information Law Practice (iLP), a law firm that is experienced in carrying out data protection audits and health checks in the education sector and beyond. Please visit www.ilp.legal or www.theisba.org.uk

It is designed to extend and compliment the other resources available to members of ISBA that aid understanding of data protection laws and how to comply with them.

What is the scope of the health check?

The scope covers the following areas of the School.

1. Overview and the School's Information Governance System
2. Accountability
3. Data Protection Principles
4. Individual Rights
5. Specific Issues
6. IT

The extent to which other legal entities connected with, but separate to the School, are compliant, such as a separate Alumni body, a separate commercial trading entity or a separate junior school are outside the scope of the health check. However, you can ask us to carry out a health check of these entities separately.

Who carries the health check out?

Either a data protection lawyer that specialises in information law or a fully trained professional that is used to working in an independent school setting such as a Bursar or retired Bursar.

How much work is involved?

A significant amount for both the School and us! It is essential that you involve all relevant colleagues in this process and not just the data protection lead. Questions should be answered by the relevant member of staff in conjunction with the data protection lead. For example, questions relating to the admissions process should be answered by the Admissions lead.

What information do I need to provide to ISBA?

You will need to gather in and send us copies of key School documentation such as your data protection policies, in advance. You will also need to complete 6 questionnaires, in draft, in advance. We need this information no later than 3 weeks before the actual interviews/visit.

How long does it take?

Up to 15 weeks providing all goes smoothly and there are no delays in getting information to us or other reasons that might cause a delay.

The first stage is to fix a date in the diary for the interview. At this point we tell you what information you need to provide and send you the questionnaires to complete in draft. You then have 4 weeks minimum to complete the questionnaires in draft and gather in the documentation. We must have this information at least 3 weeks in advance of the interview.

After the interview, providing there are no exceptional circumstances or unresolved queries, we aim to have your draft report with you in 8 weeks.

Will you visit us at School?

Yes, absolutely. The process involves us visiting for 1 day to carry out the interview. However, we can do this remotely if you prefer or if circumstances such as bad weather prevent us from getting to you.

How long will you be with us in School?

1 day. 10.00am to 5.00pm.

Can we conduct the interview remotely?

Usually, this can be arranged by Skype if possible. This can be ideal if bad weather or other circumstances prevent us getting to you.

Can we ask you other data protection questions?

During the interview, it is inevitable that you will want to ask questions as we go along. We will always try to answer them for you if there is sufficient time.

Is our information treated in confidence?

Absolutely. We will only use the information you share with us to carry out the health check and produce your report. It is retained for 6 years after the date at which you sign off our report. It will be handled in confidence and not shared with any third party other than those service providers that help us manage our organisation.

Is the Health Check the same as an audit?

No. The reason we are able to offer this service at this rate is because we have focussed our attention on the highest risk aspects of processing of personal data in school. However, our methodology is a refined version of a full audit so you can be confident that we have included the most important things.

The other characteristic that distinguishes the health check from an audit is that unlike in an audit where we interview all key staff over several days, in the health check, the data protection lead gathers the relevant information in from other key staff in advance of our visit. The health check interview involves just the data protection lead and up to 1 other member of staff.

The result is a fine-tuned methodology that has been beta tested in other schools but at a fraction of the cost of a full audit.

Appendix – Key Documents

The following are key documents that we require in both manual and electronic format, ***at least 3 weeks in advance of the interviews***.

Admissions

1. Pre-registration "enquiry" form (if one exists)
2. Application form, Registration Form, Acceptance Form and Terms and Conditions of the Parent Contract
3. Bursary or scholarship application forms and any conditions of award attached

Privacy Notice/s

4. The school's main Privacy Notice/s that are provided to pupils/parents, staff, alumni, governors.
5. Screen shots of any CCTV and ANPR signage at school

Consents to process personal data

Where the school relies on consent to process personal data, the consent mechanism must comply with the requirements of the GDPR including being "evidenced". Please provide us, where possible, with the following consent mechanisms/copy consent forms:

6. Parental/pupil consent to process personal data for the following purposes:
    - Marketing, including unsolicited direct marketing via electronic means and by post
    - Fundraising and development purposes
    - Use of images for any non-essential purpose such as school promotional and publicity purposes on the website, social networking platform (i.e. the school's Facebook page, Twitter feed, Instagram, Flickr etc.)
    - Sharing personal data including images with third parties for the third parties own including where the third party will use the personal data for their own purposes or jointly with the school. E.g. IAPS, third party journalists
    - Processing special category personal data for the purposes of
        i. exam access arrangements (e.g. an application for extra time);
        ii. references to employers/higher education establishments;
        iii. in the context of provision of learning support where data may need to be shared with a third - party psychologist etc.;
        iv. sharing with third party medical/health service providers, e.g. a private physiotherapy service.
    - School leavers and Alumni consent forms

Data Protection related policies and procedures

7. Data Protection Policy for Staff. (This may be a stand-alone policy or incorporated into other documents such as the Staff Handbook or Acceptable Use Policy ('AUP')).
8. Data Protection Policy for Pupils and Parents (if one exists)
9. Main Privacy Notices for (i) Pupils and Parents, (ii) Staff and (iii) Alumni.
    - If you have a separate Privacy Notice for Governors, please attach.

10. IT Acceptable Use Policy (staff only)
11. Any “Bring Your Own Device – BYOD” Policy or similar (Staff only)
12. Any Policy that relates to the exercise of individual legal rights under data protection law. E.g. Subject Access request Policy
13. Policy on the Retention and deletion of records
    - And any Retention and deletion schedule you use
14. Policy and or Protocol relating to Personal Data Breaches
15. Pupil Images Policy (i.e. any document that explains to pupils and parents how the school will use their images and video in any context)
16. Any policy relating to the use of personal data on the website or a school social networking platform such as Twitter or Facebook, Instagram, Flickr, YouTube

17. Screen shots of any CCTV and ANPR signage at school

Sharing personal data with third party Processors

18. Up to 2 sample contracts with processors. We suggest you send us
    - A copy of the contract with the company that hosts/supports your main pupil MIS e.g. iSAMS, SchoolBase, Capita SIMS etc.
    - A copy of any contract with a confidential waste/ data destruction company.