Data Protection Governance Framework

Compliance with GDPR

Frequently Asked Questions

Version 1 - 8/12/17
Version 2 – 27/3/18
Version 3 – 19/4/18

Questions listed are those that have arisen during the GDPR sessions or sent directly by schools to CBICT. Information provided below with (ICO) indicates advice obtained directly from the ICO.

We will update this FAQ periodically.

General information on GDPR requirements

1. **Will organizations be fined if a breach is reported after the 72 hours deadline from when the breach is discovered?**

   (ICO) It is down to the Case Officer to consider the circumstances of the breach and the causes for the delay in reporting it. The ICO will give guidance and provide information for the duration of the investigation which follows a report.

2. **Will Ofsted check for GDPR compliance with schools as they do with SCR?**
   No information has been published about Ofsted's intention regarding GDPR.

3. **Do all reported breaches result in a fine?**
   As far as DPA is concerned, not all data breaches have resulted in a financial penalty. It depends upon the organization's (Data Controller's) circumstances in terms of the details of the breach and what risk assessments, processes and procedures including policies for data protection are in place.

Schools position as a Data Controller

4. **The Data Controller – is this the school or a person? Is a person liable personally? Would schools need to take out an insurance policy to cover and protect against fines resulting from a breach?**

   In terms of the GDPR (and the DPA), the Data Controller is regarded as the school as a whole. Individuals within a school may act with the responsibilities of making decisions about what data is required to be held and how it should be processed and will engage with suppliers/providers to enable this on behalf of the school.
   There will be individuals within the school who work with the data (processing it) but effectively they each represent the Data Controller school. A person will only be liable if as a result of an investigation into a data breach, the individual has been found totally negligent in adhering to the school's data security policies.
   The ICO are lenient toward any organization who can evidence that all the GDPR requirements are in place and have taken all the necessary steps to ensure that risks for potential data breaches have been fully identified, assessed and mitigated. Fines will be applied in relation to the nature and severity of the breach in the context of the school's data protection practices and how the school ensures adherence to them. A school should consider very carefully whether an insurance policy is necessary if they are able to follow and action the recommendations for compliance with the GDPR.

Data Processors (service suppliers/software providers)

5. **Do schools need contracts with Photographers, ParentMail, RM, SIMs, Library Software suppliers etc?**
   When should schools ask Processors to confirm that they comply with the GDPR?

   Yes. Schools will need to have a contract for each of their 'suppliers' who act as Processors. A number of the main software suppliers to schools should be/are already thinking about drafting up a contract which they can use with all their client schools. The main suppliers are working with the DfE to ensure consistency. So we should see suppliers release these contracts over the next few months.

   With regard to smaller suppliers (e.g. Photographers etc.), it would be prudent for schools to ask their providers/suppliers whether they are considering drafting up a contract for use with their client schools as a prompt for compliancy with GDPR.

   (ICO) Through these contracts, schools should be assured that Processors have safeguarding procedures in place and are satisfied that Processors are processing the data in the right way.

6. **Where does a school stand regarding position of parents taking photographs at a school event (e.g. Christmas performance)?**

   (ICO) If the school itself is taking a video or photographs of children for wider publication (i.e. via a DVD, website, social media) then the school must be able to demonstrate a lawful basis for processing photos with evidence of consent which has been clearly and affirmatively given by the parents of the children involved.
   If the school has asked for consent for photos/video of their children to be used in this way as part of their yearly process (i.e. within a new starter form, or update form), then the school should keep a record of this consent given or otherwise to ensure that the school can monitor which pupils can be photographed/videoed.

   Where parents are taking photographs/videos themselves at school events, the school should decide on which approach to take. Section 36 of the DPA provides an exemption if the photos/videos taken by parents of their own child(ren) are for personal use only and if used outside of this (i.e. on social media) then this constitutes a breach unless the school can demonstrate that consent from every parent (of other children included in the photo/video) has been clearly given as an affirmative action.
   Schools could follow a higher standard for consent by seeking consent from all parents regarding video/photos under a school organised activity for recording/photographing a performance or event. This enables the school to monitor the process carefully by removing a child or children when consent has not been given.

   Please refer to the ICO guide on *Taking Photographs in Schools*.

7. **Can schools send books home with photos of other children?**

   If a school has given due consideration as to whether sending home photos of other children is necessary under the legal basis of public interest and legal obligations, then the school must have **explicit consent** from parents to share their children's photos with other children/parents in this way. We recommend that photos of other children should not be sent home.

8. **If a company providing helpdesk services uses remote access to a school's system, are they in breach of the GDPR? (E.g. HCSS access staff contracts)**

   If the company/provider uses remote access to enable them to fulfill the functions of their support contract with the school, then the company/provider needs to include this within their Processor contract with the school and be explicit about how they adhere to confidentiality when viewing schools' data in undertaking their obligations to provide support. The school needs to be assured that the company/provider have put in the necessary measures and procedures to maintain confidentiality as well as deal with breaches in their own organization.

9. **What if a Data processor ceases trading? What happens to all the data they store?**

   The Data Processor must have processes in place to protect and return or erase data in such an event. These processes must be outlined in the Data Controller-Data Processor contracts and within the Data Processor Privacy Notices. The Data Controller (school) must be satisfied that when the end of provision of services is reached, the Data Processor has enacted the processes outlined concerning return of or deletion of data.

10. **Could our PTFA use our catering company's ParentPay account to contact parents via email? Can the school use the account too?**

    This answer is based on the assumption that ParentPay collects email addresses directly from parents. The PTFA would need to enter into a specific data sharing arrangement directly with ParentPay. If this was enacted, ParentPay as the Data Controller in this relationship would need to seek consent from parents for their emails to be shared with the PTA if the use of email addresses in this way goes beyond their legitimate interest and purpose for holding the data.

    If the school wished to use the email account collected separately by ParentPay, then the Data Controller (ParentPay) contract/privacy notice needs to identify the purpose of collecting the email account and how it will be used by the school (Data Processor). As good practice, the school should also inform its parents the purpose for which email accounts from ParentPay will be used by the school within its own Privacy Notice.

11. **If a school terminates a contract with a Data Processor, is it possible to remove access to the MIS? Should it be in their contract that they will delete/remove the data previously shared with them?**

    Any data sharing arrangement can be terminated in Integris simply by clicking on the ***Remove Access*** button for any third party software that has previously been granted access. You should notify the partner when you withdraw access to your data and discuss with them whether the data for your school should be kept or removed from their systems.
    Your school should be assured about the processes the Data Processor will follow when your contract with them terminates outlined in either their Privacy Notice or contract with the school.

12. **We use CPOMs system to record safeguarding information and incidents concerning pupils. When pupils move schools, we can use its CTF functionality to transfer data to the next school**

the child moves to. If this information is requested through a SAR, should we share?

Any sharing of data must be undertaken through secure means and schools sharing such information need to ensure that the receiving school has been alerted to such information being sent to them so that they can be ready to receive it and deal with it in a secure manner.
Schools must be considerate of the safety and well being of the child at all times and the level of risk of harm to the child when considering SARs that involve safeguarding information. Schools should adhere to the guidance outlined in *'Information Sharing: Advice for Practitioners providing safeguarding services* at https://www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice

Requests for pupil information

13. **Where do schools stand regarding requests from PTA/Parents asking for names of children in classes for invites to school disco/event /birthday parties etc?**

(ICO) Schools should not give out any information relating to class lists. Parents are only entitled to view information about their own child. Publicity for events run by PTA and/or parents should be done on the basis that no specific information about pupil names can be obtained through the school.

14. **The school nurse asks termly for a list of children and dates of birth. We currently give them a class list.**

This information is necessary for the school nurse to undertake the duties required of the school nurse during their visit to the school. The school can ask themselves the question as to whether the information being requested is being shared in the most secure way. Can the school apply better controls on what and how information is being shared?
Regular visitors to the school that require pupil information to perform a function can be asked to signup to a school's **Acceptable Use Policy** which outlines the conditions, rules and agreement that visitors must adhere to when information is shared with them.

15. **What is the school's position with regards to Ofsted asking for a list of medical conditions relating to pupils on a school inspection visit?**

In Ofsted's official capacity, Inspectors can ask for information relating to pupils and staff in the course of their inspection. The school should ensure that the process of issuing and returning personal information from/to the school is undertaken in a secure and controlled manner within data protection guidelines.

Paper records in schools

16. **Do our Medical Conditions emergency information sheets about pupils on a notice board in our staff room breach GDPR?**

(ICO) Yes, this would constitute a breach. Schools need to ask themselves whether it is necessary for this information to be permanently on display – could this information be held in a less visible way? Could it be accessed through the MIS when needed? Medical information is regarded as 'sensitive' category data and therefore needs to have more robust procedures in place to ensure it is protected. Schools must be able to demonstrate that they have considered what is the most appropriate and secure way to hold this information.

17. **Should schools still maintain a pupil signing in/out book in open display at reception?**

    (ICO) Recommendation is that the signing in/out book should be kept securely if possible although it can sometimes be determined by the logistics of the reception area. Schools should look carefully at whether 'reasons for absence' should be included. If a school can justify reason for including reasons in the sign in/out book, then the book must be out of open display and held securely.

Physical Resources

18. **What is the situation regarding the use of iPads and laptops for personal use by staff?**

    It is the decision of the school. Internal safeguards should be in place to prevent improper use along with Acceptable Use Policies which staff must sign up to. The AUP should clearly state the do's and don'ts regarding IT/Internet use and acts as a 'contract' between the school and staff members. Staff can be held to account if the AUP is not adhered to.

19. **What liability exists regarding loss/theft of devices from homes or cars? (e.g. laptops left in cars)**

    There will always be risk of theft or loss of any device from the home or car. The ICO recommends that the device, if used for holding personal and/or sensitive data, should have all the data stored on the device encrypted. This significantly reduces the chance of unauthorised or unlawful processing of the data in the event of loss or theft.

20. **Should every file containing sensitive data on a staff laptop be encrypted? Is it enough to have one password to login?**

    As with above, school needs to be reassured that any personal data stored on a staff laptops are encrypted to significantly reduce the risk of unlawful exposure in the event of loss or theft. Having **effective** passwords to login to the device should be a normal undertaking but not the only method of protection deployed. Schools need to ask whether it still remains necessary for staff to hold pupil information on laptops and whether, with the advent of cloud based systems, information can be accessed more directly and securely?

Sending information/data

21. **What are the guidelines for transferring data onto other schools?**

    The DfE and the LA have provided secure transfer systems for sending CTFs and other files securely from school to school and between the LA and schools (S2S, Anycomms). Any standard CTF file should be exchanged through these systems.

    If additional files containing personally identifiable information have been created by schools themselves (primarily spreadsheets), then these files should be sent where possible through the Anycomms or S2S routes.
    Where files are sent to external suppliers/providers, please refrain from sending files as attachments to emails as this is NOT secure and breach the GDPR. Suppliers/providers should be able to provide their own secure method for sending files to them (and this should be outlined

in the Controller-Processor Contract).

22. Can we continue to send yellow folders onto the next school?

The yellow folders will contain different types of information relating to an individual pupil and will vary from school to school. The name of the child will be included and this allows the pupil to be personally identifiable from it. Therefore, schools must consider how the yellow files are transferred to the next school (i.e. in person) and the extent to which personal and sensitive information is included within them. Really, they should not contain any personal or sensitive information in them regardless of how they are sent onto the next school.

23. **Is password protection on documentation necessary when emailing?**

Confidential information held in documents with PII and/or sensitive data should NOT be sent as attachments through emails.
Documents/files can be sent between schools and the LA using Anycomms secure data transfer system (HT's have their own personal user account for the transfer of confidential information).
If you use any support services, they should provide you with their own method of secure transfer with their service (which should be outlined in their contracts).

The school can make a decision as to whether adding in a password to protect the document is adequate when considering the nature and content of the document being emailed. However, password protection is a low level of protection.
Encryption of documents should be considered if there is no available data secure transfer mechanism available.

Collection of information

24. What is our position regarding emergency contact details provided by the Data Subject (i.e. a parent/carer of a pupil)?

The school should make it clear that the Data Subject providing emergency contact information to the school has done so on the basis of seeking agreement from the individuals concerned. The school can use a form of acknowledgment from the parent/carer that this has been done. The updated New Starter form includes this additional condition and acknowledgment.

25. How often should a school re-apply for informed consent?

Consent is necessary when the personal information being asked for is not based on a legal obligation or public interest. If the original request for information was not felt to be made in a fair, clear and transparent way, then a school may re-apply for informed consent.
Additionally, if a data item e.g. a parent's email address, has been obtained for the purpose of emergency contact but has been subsequently used by the school for additional purposes (e.g. marketing), then the school should apply to the parent for consent for the email address to be used in this way. It is important that the school is being transparent in how the data collected is being used.

Subject Access Requests (SARs)

26. Can data subjects see safeguarding documents?

This is a decision that the HT must make based on the guidelines within the *Keeping Children Safe in Education*. The current ICO guidelines within the *SAR Code of Practice* stipulate that information should **not** be shared if: it might cause harm to the physical or mental health of a pupil or another individual; reveal that the child is at risk of abuse; disclosure of information would not be in the child's best interests; information contained in adoption and parental order records; certain information has been given to a court in proceedings concerning the child.

Disposal of information and physical resources

27. What needs to be shredded (e.g. children's paintings with their names on them)?

Any paper records or items which contain any personal information should be disposed of securely if the original item (e.g. painting) has not been returned to the child.

School Staff

28. Is it worthwhile to have full staff training on GDPR, so that everyone knows their responsibilities? Should this be done by a GDPR Practitioner?

Staff should be aware of their responsibilities under GDPR and briefing sessions or specific training is a good way of keeping data protection at the forefront. Schools can elect to include data protection training alongside Safeguarding training/induction. Briefing sessions for staff should be delivered by someone who is knowledgeable about the GDPR requirements and how it impacts on schools. Seeking an external individual with GDPR Practitioner status provides this assurance.

29. How can we ensure that staff who have left the school have not retained any information at home? If there is a data breach once they are no longer employed, is the ex staff member liable?

If a data breach case is brought against the ex-member of staff concerning personal information held by the school, then the individual is liable. The school however, is in a much stronger position to enforce its rights if there are clear and concise policies in place regarding use of personal information and staff obligations under the GDPR. Using Acceptable Use Policies (AUPs) for staff makes these obligations for staff very clear.

30. Can staff take student named books for marking, seating plans etc. out of school?

If this is the agreed practice for the school, then the school must ensure that data protection policies and procedures are adhered to and that any devices/data are appropriately encrypted to protect personal information. A school can include the school's conditions for protecting personal information in an Acceptable Use Policy for staff.

Governing /Trust Boards

31. **Ultimately, Governing or Trust Boards are accountable for the school's compliance. In the case of MAT Trustees, who are directors and have the same kind of liability as commercial directors, would they be individually liable for financial penalties in the event of a data breach?**

    In terms of the GDPR, it would be a corporate liability of the company rather than individual directors in any event. The limited liability status of the charity would mean the corporate veil would protect the directors individually. (E.g. charities have been fined for sending 'begging' messages for money to individuals who never consented for their phone numbers to be used in this way. The charitable organization receives the fine and not the individuals causing the data breach).

32. **What would be the position if we used one of our Governors to undertake the data protection officer role in terms of leading and guiding the process?**

    Governors have a specific responsibility to monitor and review the school's processes for compliance with the data protection regulations and need to ensure they factor into their review cycle opportunities to do this effectively. Having a Governor leading on the school's processes is a clear conflict of interest and therefore, we would not recommend schools take this approach.