**Oxford Diocesan Schools Trust**
St Mary's Convent, Denchworth Road, Wantage, Oxfordshire OX12 9AU

# ODST Guide for Local Governing Body Members: GDPR

## What is the GDPR?

The UK's General Data Protection Regulation (GDPR) came into force on 1 January 2021. It sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies.

It is based on the EU GDPR (General Data Protection Regulation (EU) 2016/679) which applied in the UK prior to this (when the UK was part of the EU; with some changes to make it work more effectively in a UK context.

The UK's Data Protection Act 2018 (UK DPA 2018) sits alongside the GDPR and tailors how GDPR applies in the UK; this is covered in Part 2 of the Act (Parts 3 and 4 cover law enforcement processing and intelligence services processing, respectively).

## Data Protection

Data protection is about ensuring people can trust that their personal information is being used fairly and responsibly. The UK's GDPR and Data Protection Act 2018 take a flexible, risk-based approach to data protection, based on some key principles.

The onus is on organisations to think about, and justify how and why, they use personal data. Every organisation is different and there is no one size fits all answer. Data protection is not, and should never be seen as, a barrier to innovation.

## What does GDPR mean for schools?

Schools need to comply with the GDPR, and, in theory, this should mean a review and strengthening of existing data protection practice, rather than a need to start at the beginning.

It is important to regularly review data protection policies and procedures and ensure that data processing is in line with the key principles set out in the GDPR. These principles are:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

They should lie at the heart of how any individual's personal information is used in all schools.

## Children and GDPR

The GDPR explicitly states that children require specific protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards, and also their rights in relation to the processing of personal data.

In the 'what else needs to happen' section (page 22) of her report, **'Who knows what about me?'** (November 2018), the previous Children's Commissioner, Anne Longfield, recommended that:

*"Schools should teach children about how their data is collected and used, and what they can do to take control of their data footprints. These lessons should cover information shared online but also gathered in the home (e.g., through connected devices) and outside the home (including through public services)."*

The report also includes 'Ten top tips for children and parents' (page 23) which schools could find useful, and there is an infographic available through the link above which gives a good visual summary.

## What should governing boards do?

For governing boards, the role is to:

- ensure that good data protection practice is embedded into the culture of the school/academy/trust they govern
- monitor arrangements in place in relation to data protection, especially regarding the GDPR key principles
- be satisfied that the necessary steps have been taken/or are being taken to ensure compliance with the GDPR and the UK DPA 2018
- ensure there is a training programme in place for all staff and governors, including any new members as part of their induction.

## With this in mind, governors should:

1. Be aware that ODST have a **Data Protection Officer:**

   DPO - Mike Bingham, Operations Manager, ODST, mike.bingham@oxford.anglican.org, Dpo.odst@oxford.anglican.org
   07342 997243.

   The role of a DPO is to independently and objectively advise the school leadership and staff about their data obligations, monitor compliance, advise on when data protection impact assessments are needed, and act as a point of contact for communication with the Information Commissioner's Office.

The DPO will need to be able to report directly to the highest level of management in the school.

2. Check whether a **data asset register**, or equivalent, has been drawn up and is regularly reviewed and updated as necessary.

3. Check up to date **privacy notices** are in place and published, and they are periodically reviewed.

4. Review and update relevant **policies and procedures** to reflect any changes in legislation as well as practice in school.

   Key policies and procedures are:

- Data Protection
- Subject Access Request
- Data Breach Procedure
- Data Protection Impact Assessment
- ICT policies including:
  - E-safety
  - IT security
  - Acceptable user agreements
  - Use of social media
  - Website requirements
- Information Security and Business Continuity
- Codes of Conduct
- CCTV Policy (if applicable).

5. Ensure **training needs** have been identified and that a programme is in place for staff and governors. Ideally, there will be a blended approach with face to face/online training delivery, updates on INSET Days (linked to safeguarding works well), reminders/sharing of learning opportunities in staff meetings, newsletters, emails etc.

6. Consider appointing a **Data Protection Governor** to be the link with the school Data Protection Lead, or DPO, and ensure that the governing board fulfils its data protection responsibilities.

   It is recommended that the Data Protection Governor undertakes regular school visits to meet with the school's Data Protection Lead.

7. **Scrutinise** – LGB members should monitor and evaluate the application of existing policies and processes that relate to data protection. Data Protection should be a regular agenda item (this can be at committee level).

**Some data protection questions governors could ask**:

- What is the impact on the individual of any new policy, system or initiative?
- Has a Data Protection Impact Assessment been carried out to assess any risks to personal data and identify actions that could be taken to reduce these?
- Can it be demonstrated that the GDPR principles have been considered and met? (Undertaking a DPIA is a great way of evidencing this)
- Have the risks associated with any processing of personal data been identified? What has been done (or will be done) to mitigate any risk, or bring it to an acceptable level?
- Are individuals given information about how their personal data will be used by the school/trust when it is first collected, as well as what their rights are in relation to this (this is usually via access to the privacy notices)?
- Is the school/trust confident that any suppliers/contractors are GDPR compliant?
- Are there data sharing agreements in place covering any regular sharing of personal information (such as with external professionals/agencies)?
- Have there been any subject access requests (SARs); were they dealt with in line with the school's procedure?
- Have there been any data breaches or potential data breaches; were these dealt with in line with the agreed procedure; what actions were taken; were there learning points for the future and have these been shared with staff?
- Is everyone's data protection training up to date?

NB: Ensuring scrutiny is evidenced in minutes is an excellent way of demonstrating the Board's accountability in relation to the GDPR, which is one of the key principles.

**Sanctions**

Data protection law is not about fines; it is about protecting the rights and privacy of the individual and making organisations accountable for protecting those rights and privacy. Whilst the ICO has the power to issue fines; they are only issued as a last resort and do not fund the work of the ICO.

In 2018, Elizabeth Denham, the Information Commissioner at that time, said:

*"It's scaremongering to suggest that we'll be making early examples of organisations for minor infringements or that maximum fines will become the norm. The ICO's commitment to guiding, advising and educating organisations about how to comply with the law will not change under the GDPR. We have always preferred the carrot to the stick."*

## Implications for LGB members as individuals

LGB members should consider using an email address issued by the school for governor business. When sending personal data/information (e.g., pupil exclusion letters) by email, personal data should be kept to a minimum in the body of the email (use initials rather than full names) and attachments should be encrypted or password protected. Any hard copies containing personal information circulated at meetings should be returned to the school at the end of the meeting for safe disposal.

When LGB members reach the end of their term of office, any information they have at home should be returned to the school for disposal/safe keeping.

Schools could consider using a GDPR-compliant cloud platform for access and storage of governing board documents that can also be used as a communication tool by LGB members. This strengthens data security through a reduction in the use of emails, which is where accidental disclosure of personal data occurs most commonly across all organisations, including schools.

For any hard copy documents, the school could consider offering the governing board a secure facility (such as a drawer in a lockable filing cabinet) for the storage of any documents that contain personal data. It would be important to record this in the school's data asset register to ensure that this is monitored, and the data dealt with appropriately.