PARTNERS for EXCELLENCE
BRENT SCHOOLS PARTNERSHIP

Services to schools

General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA)

1st April 2020 – 31st March 2021
Service

The General Data Protection Regulation (GDPR) came into force across Europe on 25 May 2018. This service is being made available to schools to ensure compliance with the regulation and the Data Protection Act 2018 (DPA).

Quality Assurance of services is a key priority for the BSP. All designated Data Protection Officers appointed through BSP have achieved Certified Information Privacy Professional/Europe (CIPP/E) or Certified Information Privacy Manager (CIPM) accreditation. CIPP/E and CIPM were developed by the International Association of Privacy Professionals (IAPP) and CIPM also holds accreditation under ISO 17024:2012

Introduction

The General Data Protection Regulation (GDPR) was adopted by the European Parliament on 27 April 2016 and the ensuing Data Protection law came into force across Europe on 25 May 2018. On 23 May 2018, the Data Protection Act 2018 (DPA) received royal assent and became UK law. The DPA 2018 replaces the DPA 1998 and implements the GDPR, while providing for certain permitted derogations, additions and UK-specific provisions.

Schools that complied properly with the DPA 1998 have found that much of their approach to compliance has remained valid under the DPA 2018.

However, there are new elements and significant enhancements including:

- Greater **accountability** through the statutory role of the Data Protection Officer (DPO)
- Increased **transparency** requirements (enhanced privacy notices and a new Record of Data Processing Activities)
- **Reduced timeframes** for Subject Access Requests (SAR) and penalties for failure
- **Compulsory notifications** for data breaches (normally within 72 hours)
- Privacy by design, involving carrying out **mandatory Data Protection Impact Assessments** (DPIA)
- **New rights** for individuals, and strengthening of existing rights
- Requirement to **demonstrate compliance**, including evidence of staff training, compliance assessments and audits
- Regular **enhanced monitoring** of cyber security
- **Higher penalties** for non-compliance (maximum fine increased from £500,000 to £20m)

The new approach can also be broken down into four Rs:

1. **Reviewing** your Data Protection policies
2. **Refining** your data processing procedures
3. **Recording** your data processing activities and the legal bases for those activities
4. **Reporting** outcomes of impact assessments, audits and investigations

As part of their statutory duties and obligations as Data Controllers and public authorities, Brent schools are required to designate a Data Protection Officer (DPO) in order to comply with the GDPR and the DPA 2018. A school may designate an internal DPO from existing staff, or designate an external DPO to act for a group of schools. The DPO is responsible for managing compliance with the school's Data Protection Policy.

Brent Schools Partnership offers an overarching Data Protection service to help schools fulfill their duties and obligations as Data Controller. A key part of this service is the designation of a named Data Protection Officer (DPO).

The Data Protection service is available to BSP members at the following rates:

Primary School with **up to 250** pupils on roll	**£1500** per annum
Primary School with **251 or more** pupils on roll	**£2500** per annum
All-through and Secondary Schools	**£3500** per annum

(Please note: individual schools within a MAT will be required to pay separately for the service)

BSP provides a bespoke service which meets the specific needs of your school, and level of your schools existing GDPR compliance. The BSP package includes one-and-a-half-day entitlement of support from your DPO. This can be comprised of three 0.5 days, the focus of which will be agreed with your DPO at the start of the year.

The package includes the following strands:

- A designated Data Protection Officer (DPO) for the school who is
  - the notified individual to the Information Commissioners Office (ICO) and published within a public register;
  - the named individual for direct contact by Data Subjects
- A suite of GPDR compliant model documents (Policies; Procedures; Forms; Privacy Notices)
- Whole staff training materials
- Termly training/briefings for key school staff
- Review of the school's data sharing agreements
- Supported self-assessment for DPOs - **0.5-day equivalent** by telephone and email
- Compliance visits to review self-assessment and quality assure self-assessment of DPLs - **0.5-day equivalent** on site
- Compliance - **0.5 day visit** to provide an annual review of procedures and implementation
- Data Protection Impact Assessments (DPIA) for new projects
- Correspondence with ICO as and when required
- Logging and tracking of Subject Access Requests (SAR)
- Data Breach investigations (including correspondence with ICO and report to school)
- Termly Information Governance reports to schools
- Data Protection advice and guidance by telephone and email
- Networking opportunities for staff with Data Protection responsibilities

The Role of the Data Protection Officer
(adapted from Information Commissioners Office guidance)

What are the tasks of the DPO?

The DPO's minimum tasks are defined in Article 39:

- *To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws*
- *To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits*
- *To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, pupils and parents)*

What does the GDPR say about employer duties?

Schools must ensure that:

- *The DPO reports to the highest management level – i.e. leadership team and governors*
- *The DPO operates independently and is not dismissed or penalised for performing their task.*
- *Adequate resources are provided to enable DPOs to meet their GDPR obligations.*

Can schools allocate the role of DPO to an existing employee?

Yes, as long as the professional duties of the employee are compatible with the duties of the DPO and do not lead to a conflict of interests – i.e. not Headteacher, Deputy Headteacher, Business Manager or Data Manager.
Schools can also contract out the role of DPO externally.

Does the data protection officer need specific qualifications?

The GDPR does not specify the precise credentials a data protection officer is expected to have.
It does require that they should have professional experience and knowledge of data protection law. This should be proportionate to the type of processing your organisation carries out, taking into consideration the level of protection the personal data requires.

Note: Brent Schools Partnership believes that Quality Assurance of DPOs is critical in giving schools confidence in effective Data Protection compliance. Designated DPOs appointed through BSP have achieved Certified Information Privacy Professional/Europe (CIPP/E) or Certified Information Privacy Manager (CIPM) accreditation. CIPP/E and CIPM were developed by the International Association of Privacy Professionals (IAPP) and CIPM also holds accreditation under ISO 17024: 2012.

For further information, please contact:

Matthew Lantos (matthew.lantos@bsp.london)