Schools' Compliance with GDPR

Overview

Overview of GDPR for schools

- From 25th May 2018: EU GDPR Single personal data privacy law enforced across EU
- **From 1st Jan 2021 (after Brexit): UK GDPR affects ALL organisations in UK**
  Updated Data Protection Act 2018 (reflecting UK law enforcement and intelligence agencies)
- Personal data relates to **Personally Identifiable Information (PII)** relating to an individual who is the **Data Subject**.
- PII data also includes IP addresses, biometric data, mobile device IDs and website cookies. Some of this data is categorized as 'Sensitive Data' – for schools this is ethnicity, religion and health information
- All organisations must have a legal basis for holding personal information. The legal basis for schools to hold pupil and staff data is under Public Interest and a legal obligation (in order to submit statutory returns to the DfE). The pupil and staff data items held is listed within the Common Basic Data Set (CBDS). Any personal data held outside of the CBDS list can only be obtained through consent from parents/carers

- **Data Subjects** have a set of rights and can request through a **Subject Access Request (SAR)** the right to access information – i.e. a parent/carer has the right to request access to their child's information held
- Two principal roles within GDPR – **Data Controllers** and **Data Processors**
- Schools are **Data Controllers** as they determine how and why personal data is to be processed and used
- Service provider/external third-party suppliers who processes the data on behalf of the Data Controller (schools) through agreements/contracts are the **Data processors**. GDPR requires schools to have Controller-Processor contracts for each supplier.

- The Independent governing authority - **Information Commissioner's Office** (ICO) – monitors organisations' behaviours regarding data protection and deals with all complaints referred to them
- UK GDPR focuses more intently on prevention of data security breaches and misuse/loss of personal data. Organisations are held more accountable for their practices relating to data protection and served with heftier fines for data breaches depending on their level of severity.

- **GDPR Leads**: Schools must have an identified GDPR Lead who monitors compliance and champions data protection.
- Schools are expected to review current practice and revisit and update all policies relating to GDPR. [*CBICT's **Data Protection Governance Framework** provides policy template resources for schools subscribing to this service*]