**Overview of GDPR**

* GDPR is enforced on May 25th 2018 which allows time for schools to prepare for it
* Single EU data privacy law which is a strengthening of the current Data Protection Act and focuses more intently on prevention of data security breaches and misuse/loss of personal data. Organisations will be more accountable with heftier fines for breaches
* 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
* Two principal roles within GDPR – Data Controllers and Data Processors
* The Data Controller is the school who determines the why and how personal data is to be processed
* The Data Processor is the service provider/supplier who processes the data on behalf of the Data Controller - in the case of schools, it is the software suppliers that the school has contracted. GDPR requires the schools to have Controller-Processor contracts for each supplier.
* 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 record
* The legal basis for schools to hold pupil and staff data is under Public Interest and a legal obligation to make statutory returns.
* The range of pupil and staff data held is listed in the Common Basic Data Set (CBDS) for each. Look at *Annex B* in Central Bedfordshire Data Sharing Agreement for a list of the data items.
* Any personal data over and above the CBDS can only be obtained through consent from the parents/carers
* Consent must be clearly explained and must be an affirmative action by the parents/carers
* Data Protection Officers can be employed although not a requirement. Schools need to have an individual who is leading on GDPR compliance and who will champion data protection once the regulations are enforced in May 2018. Schools can if they wish group together to employ a Data Protection Officer or employ services of an external provider who can audit the school’s data protection procedures to ensure compliance.
* Schools are expected to review current practice and revisit and update policies. CBICT recommend schools follow the procedures within the **Data Protection Governance Framework** to start work toward compliance.