The St Marylebone CE Bridge School
A Special Free School for pupils with Speech, Language and Communication Needs
Herries Street, London W10 4LE

GDPR Guidance for Governors on Handling Personal Data

Author:	Kate Miller
Last reviewed:	**July 2023**
Review cycle:	**Annually**
Approval at Plenary required?	**No**
Required to publish on website?	**No**
Statutory:	**No**

Context:
As part of a review of data protection policy, St Marylebone Bridge needs to provide Governors with advice on the handling and storage of personal data covered by UK data protection law (UK GDPR) All Governors should familiarise themselves with the School's Data Protection Policy which can be requested from the Clerk to Governors.

Personal data is defined as: any information relating to a living individual who can be directly or indirectly identified from it. This includes name, address, contact details but could also include two or more non-specific pieces of information that when combined could identify specific individuals, including, for example, a combination of gender, birth date, geographic indicator and other descriptors.

1. Types of data

Governors will generally handle two types of data which fall within the remit of the UK GDPR:

- Contact details (such as email addresses) of individuals both within and outside of the School
- Personal information, including but not limited to, that provided for job applications, pay reviews, staffing updates, appeal panels, safeguarding

2. Key principles

The School's policy on Data Protection requires Governors to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure, and that, in particular, they will comply with three key principles:

- paper files and other records or documents containing personal data are kept in a secure environment
- personal data held on computers and computer systems are protected by the use of secure passwords which, where possible, have forced changes periodically.

- individual passwords should be such that they are not easily compromised.
- personal data must only be stored on school owned devices and drives such as Google drive.
- personal data must be stored and then deleted in accordance with the data retention policy.

3. Handling of data

In order to comply with the principles set out above, the following guidelines should be followed:

- Paper copies of documents containing personal data should be kept in a secure location (such as a locked cabinet or desk) and should be disposed of securely when no longer required - if necessary, they can be returned to the Clerk to Governors who can arrange to have documents shredded. Also, care should also be taken when reading confidential documents in a public place, such as a train.
- No personal data is to be stored on devices or drives that are not owned or accessed by the school.
- Where a device is shared with any other individual (e.g. family member), access to relevant data must be password protected and not accessible to that individual. Similarly, email addresses used by Governors for School business should not be shared with any other individual.
- When any electronic device is disposed of, all files containing personal data should be properly destroyed using specialist software or professional assistance, in accordance with the Data retention policy.
- Passwords should be of suitable length and complexity (a mixture of upper and lower case, numbers and symbols) and should be changed regularly.
- On stepping down from the Board, Governors should ensure that all paper copies of documents are securely destroyed or returned to the Clerk to Governors for shredding, and that all electronic files (including emails) are securely deleted.

4. Data breaches

Governors should advise the School or DPO immediately if they become aware of any loss or theft of an electronic device or hard copy papers on which personal data is held, or any security breach of electronic systems (such as through cyber-attack or malware).

5. Other relating documents

This policy relates to

- Data Protection Policy
- Data Retention Policy
- Privacy Notice Staff
- Privacy Notice Pupils and Parents
- Privacy Notice Contractors and Suppliers
- Privacy Notice Governors
- Data protection code of practice including email security

When implementing this policy the latest guidance will be referred to, even if the guidance has changed since the last policy review.