DATA PROTECTION CODE OF PRACTICE including EMAIL SECURITY

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

1. Security of personal data

1.1 Of fundamental importance within any data protection regime is the security of the personal data that is being processed. Data subjects have the right to expect that their personal data will be kept and processed securely and that no unauthorised disclosures or transfers will take place to anyone either within or outside the school.

1.2 Authorised disclosures or transfers are those that are defined within the appropriate notifications and declared to the data subject either at the point of data collection or subsequently, the necessary consent for disclosure or transfer having been obtained if required. To help ensure the security of personal data within the School, all those in theSchool who process such data are required to follow the general guidelines set out below.

1.3 Each member of staff whose work involves storing personal data, whether in electronic or paper format, must take personal responsibility for its secure storage, in line with St Marylebone Bridge Data Protection Policy.

2. Legislation and guidance

This Code of Practice is designed to meet the requirements of the UK GDPR and the provisions of the Data Protection Act 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and the ICO's code of practice for subject access requests. It is also based on the ICO guidance on UK GDPR, and information provided by the Article 29 Working Party.

It also meets the requirements of the Protection of Freedoms Act 2012, ICO's code of practice in relation to CCTV usage, and the DBS Code of Practice in relation to handling

sensitive information. This policy also complies with the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Responsibilities of Staff

3.1 All staff are responsible for the below.

(i) Checking that any information that they provide to the School in connection with their employment is accurate and up to date.

(ii) Informing the School of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The School cannot be held responsible for any errors unless the staff member has informed the School of such changes.

(iii) If and when, as part of their responsibilities, staff collect information about other people (e.g. about a student's course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff set out in the School's Data Protection Code of Practice and Data Protection Policy.

4. Data Security

4.1 All staff are responsible for ensuring the below.

(i) Any personal data that they hold is kept securely.
(ii) Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.
(iii) Sensitive data is not transferred and must only be downloaded onto devices that are owned by the school.
(iv) The teacher must not share documents containing personal information beyond the individual members of staff that need to know that information and only to individuals employed by the School.

4.2 Staff should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases.

4.3 Personal information should:

(i) be kept in a locked filing cabinet, drawer, or safe

or

(ii) If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up

and

(iii) Personal Data must not be stored on removable hard drives or on equipment not owned by The School.

4.4 Rights to Access Information

All staff, students and other users are entitled to:

(i) know what information the School holds and processes about them and why
(ii) know how to gain access to it
(iii) know how to keep it up to date
(iv) know how to delete it
(v) know how long it is being kept for.

4.7 All staff, parents and other users have a right under the 2018 General Data Protection Regulation to access personal data being kept about them or their child either on computer or in files. Any person who wishes to exercise this right should email office@stmarylebonebridgeschool.com

5. Subject Consent

5.1 In many cases, the School can only process personal data with the consent of the individual. This include the use of photographs or video. It is the responsibility of the member of staff to check that this consent has been given.

5.2 Sensitive data i.e. Biometric data can only be collected and stored with consent.

5.3 The School may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition, such as asthma or diabetes. The School will only use this information in the protection of the health and safety of the individual, but will need consent to process this data in the event of a medical emergency, for example.

6. Processing Personal Data

6.1 The School stores pupils' personal data on SIMS. If this data is extracted and stored and in another location in the school drive this must be recorded in the Data Processing record. This document will record the location of this personal information, who has access to it and for how long it is to be kept.

6.2 SLT and Key Stage Leads will hold personal data outside of SIMS on the School Drive. These must be recorded on the to the School's Data Processing record.

6.3 Where personal data is transferred between staff members **within** the School, the level of security appropriate to the type of data and anticipated risks should be applied. For example, sensitive personal data should either be transferred by internal mail or in sealed envelopes or by hand.

6.4 Staff procedures for sending pupils information on email.

(i) Personal data must not be attached to emails. Any documents for use by staff should be saved in the shared area and a link to this sent in an email. This file must only be

shared with the employees who need to use it. The access to this data is therefore password protected.

(ii) Where documents have to be attached which include sensitive data a password needs to be added. This must only be to an organisation that is GDPR compliant and with whom we have permission to share such data.

6.5 Personal data should not be processed at staff members' homes or in transit, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites. Off-site processing of personal data in manual or computerised form by staff presents a potentially greater risk of loss, theft or damage to personal data. Staff should thus be aware of both the institutional and the personal liability that may accrue from their off-site use of personal data.

6.6 In cases where such off-site processing is felt to be necessary or appropriate, the agreement of the Head of School must be obtained, and all the security guidelines given with this permission must be followed.

6.7 Staff should take particular care when laptop computers, personal machines and portable devices, such as phones and tablets, to ensure that personal data is not downloaded onto these devices.

7. Use of Email

School employees, governors, and third party staff using email to conduct business on behalf of the school, or who have access to a school email account should abide by the following guidance on email security. By doing so, this ensures that the technical IT security measures the school has in place remain robust, and are less likely to be compromised.

a) Passwords /logins to the email and IT system should be ten characters long with a mix of letters, numbers and special characters. This must not be written down anywhere.

b) Emails should be regularly reviewed, and either filed, archived or deleted if not required anymore.

c) Sensitive or Special Data, which might include SEND, EHCP, medical or health information, criminal record data or financial information, should not be sent without appropriate protection and/or encryption.

d) Carefully check the recipients of the emails they are sending, especially if the auto-complete function is operating giving suggested recipient email addresses.

e) Carefully check the recipients listed in the CC box and BCC box to ensure email confidentiality of recipients where necessary.

f) Ensure email contacts are up to date, especially those that are dated or preset.

g) Ensure all anti-virus software and malware software is up to date on your machines

h) Do not open an attachment unless you know who the sender is, or what the attachment is about.

i) Do not enable Macros unless you have checked with the IT Manager first.

j) Do not click on links to web pages without first hovering the cursor over them to see if the page looks legitimate. Consider opening a blank browser and typing the address.

k) Users must report unsolicited mail ("spamming") to the school office and/or the school IT manager by email to TariqS@joskos.com. Do not click the "Unsubscribe" link in a spam email. It would only let the spammer know your address is legitimate, which could lead to you and other users receiving more spam.

l) Email will in a user's absence be monitored or forwarded to another account for processing where necessary in the interests of business continuity.

m) When you have finished with your terminal/machine, or need to leave it for some reason, either ensure you have a timed lock out in place OR be sure to log out. Always log out at the end of the day.

n) Do not "Reply to All"

8. Other related policies

This Code of Practice relates to

- Data Protection Policy
- Data Retention Policy
- Privacy Notice Pupils and Parents
- Privacy Notice Contractors and Suppliers
- Privacy Notice Governors
- Privacy Notice Staff

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

Appendix A

The St Marylebone CE Bridge School: Data Protection Policy Staff Agreement

The St Marylebone CE Bridge School's Data Protection Policy sets out the School's obligations with regard to the GDPR and Data Protection Act 2018. All staff are expected to familiarise themselves with their obligations and responsibilities in this respect, as laid out below:

School staff are expected to:

- be aware that the data they deal with daily includes personal data about pupils and other individuals and should therefore be stored, shared and communicated in a professional and sensitive way at all times
- follow the School's Email Policy, ICT Acceptable Use Policy and Data Protection Code of Practice and data Protection Policy at all times
- seek guidance without hesitation if they are concerned about their own use of data or that of another employee.

Personal data or information is data from which an individual can be identified. This includes lists of pupils' names, references, education records, assessment data, employee information. A special category of Sensitive data referrers to Biometric data such as fingerprints or DNA.

Specific responsibilities of staff:

1. Your school login details must not be shared with anyone else.
    a. You must use a password of sufficient length and difficulty (i.e. consisting of at least 10 characters and including numbers and letters)
    b. You must change your password as and when instructed by the School's IT service.
    c. You must have a different password for your SIMS login
2. Records of personal information held in School must be protected by a password. Every member of staff has his or her own login details with pre-arranged permissions as to the access they have to personal information held in School.
3. Personal information must not be transferred to a portable device except in exceptional circumstances with written permission from the Head of School. This includes downloading information from email onto portable devices. In such circumstances:
    a. Information must never be transferred onto a portable hard drive or USB stick.
    b. Laptops, mobile phones and tablet PCs must also be password- or pin-protected
4. Personal information must not be stored on home computers. If you work from home using personal information files must only be accessed by Google Apps for Education cloud storage.
5. Emails
    a. Only send emails to the relevant recipient(s)
    b. Do not attach files containing personal information to emails. Such files can be shared via Google Drive as this requires a password and / or permissions to access.
6. School computers should always be locked when not in use. This can be done by pressing ctrl+alt+del.
7. Documents shared on the School's Google Drive should only be shared with the appropriate members of the School community.
8. Data must not be kept for longer than is necessary for its purpose. This is usually the duration of a pupil's time on roll at the School. It then should be permanently deleted or transferred to the secure school archive.
9. The School seeks the parents/carers permission to be able to use photos of their child in School materials or publications, paper or online. Staff should be aware of this list when planning trips and performances when photographs may be taken. The list is available on the portal.
10. Any requests for personal information must be directed to theHed of School.
11. Personal Data must only be stored for a set amount of time and in a known location. Staff must use the Data retention policy for guidance in this.

Declaration:

I have read and understood the Data Protection Policy and Data Protection Code of Practice of The St Marylebone CE Bridge School. I confirm that I will abide by the procedures outlined in the document.

Name: **Job title:** **Date:**