ST MARGARET'S CE PRIMARY SCHOOL

DATA PROTECTION STAFF ACCEPTABLE USE AGREEMENT

March 2025

1 Introduction

This agreement is to be read in conjunction with the school's Data Protection Policy and must be signed by new staff. (Appendix 1).

At St Margaret's School we have a shared responsibility to ensure that we take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

A key principle of the General Data Protection Regulation (GDPR) is that we process personal data securely by means of "appropriate technical and organisational measures" – this is the "security principle". This means that we must have appropriate security to prevent the personal data we hold being accidentally or deliberately compromised. This includes personal data on paper as well as in electronic form.

2 Rules to sharing information

The seven golden rules to sharing information:

1. Remember that the General Data Protection Regulation (GDPR), Data Protection Act 2018 and human rights law are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately

2. Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so

3. See advice from other practitioners, or your information governance lead, if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible

4. Where possible, share information with consent, and where possible, respect the wishes of those who do not consent to having their information shared. Under the GDPR and Data Protection Act 2018 you may share information without consent if, in your judgement, there is a lawful basis to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be clear of the basis upon which you are doing so. Where you do not have consent, be mindful that an individual might not expect information to be shared

5. Consider safety and well-being: base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions

6. Necessary, proportionate, relevant, adequate, accurate, timely and secure: ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (see principles)

7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose

Appendix 1

To ensure that we comply with the "security principle", the school has set out a list of measures that we must all adhere to:-

Staff must:

- Read the Data Protection Policy (on school website)
- Ensure that confidential paper records are kept in locked filing cabinets or cupboards
- Ensure that confidential paper records are not left unattended or in clear sight anywhere in the school that has general access, including unattended classrooms and offices
- Ensure they have permission from the school before removing any personal data from the building or taking it home
- Ensure that any personal data that has been taken home is locked away when being stored
- Use secure remote access when working away from school
- Use the Bcc option when emailing a large number of recipients or sending a circular email to parents
- Ensure that paper based, personal data and/or laptops are kept close by and stored securely when taken offsite and not left unattended. Care should be taken in public places eg. if reading personal data on a train or bus
- Ensure that any personal data transported by car is locked in the boot during transit
- When returning paper based personal data back to school, dispose of it or store it security if no longer needed
- Staff must follow the Data Breach Security Management process by reporting the loss of any paper based data, portable computing device or unauthorised access to personal information to the Data Protection Officer (DPO) as soon as possible
- Ensure that all email and postal addresses are checked to ensure the safe dispatch of information. If sending personal data by post, mark the envelope "Private – Contents for Addressee only"
- Ensure that only the required information is posted to the recipient
- Where possible, use pseudonyms/initials and anonymise personal data
- Use school devices to take photos and videos of children rather than personal devices

Staff must not:

- Take any personal data to a place of entertainment or public place such as a pub or cinema, unless it is required as part of an official school visit
- Copy other parties unnecessarily into email correspondence. Unless it is required, do not use the "Reply All" option when responding to emails
- E-mail documents containing personal data to their personal email accounts/personal computing devices
- Leave their computers unlocked or share their passwords with any other individual
- Store work related personal data/documents on their own home computers
- Print off documents containing personal data unless absolutely necessary
- Leave any documents containing personal data unclaimed in or on any printer or photocopier
- Leave personal data out on a desk overnight or away from a desk. Lock the door if this is possible
- Leave personal data in a vehicle overnight
- Discuss issues regarding personal data at social events or in a public place
- Dispose of personal information/data in non-confidential bins

- Use unencrypted USB storage devices or laptops or devices that are not password protected

I have read, understand and agree to the points in the above policy. I also understand that I have a responsibility to ensure that any personal data that I process is done so in a secure manner and not disclosed to unauthorised third parties.

Staff Name: _____

Signed: _____

Date: _____