



## **GDPR information sheet for all staff**

**Review Date: September 2023**

**Next Review Date: September 2024**

# Staff cheat sheet: how to keep personal data safe

---

**Personal data:** any information relating to an identifiable living person, e.g. name, contact details, ID numbers, attendance and assessment information, financial information

**Sensitive personal data:** includes information that reveals someone's ethnic origin, political opinions, religion, sexuality or health. In our school, it also means safeguarding information, and

## DO

### ✓ Remember that data protection laws DO NOT stop you from reporting safeguarding concerns

- You must still report to the relevant people where you're concerned about a child. You do not need anyone's consent to do this

### ✓ Only collect the information you actually need

- When you're requesting information (for example, via consent forms, admissions forms or surveys) ask yourself "Do I really need this? What will I actually use it for?"
- If you don't need it, or only want it "just in case", don't collect it
- If you've already collected personal information that you don't need, delete it

### ✓ Keep personal data anonymous, if possible

- For example, if you're emailing a colleague about accommodating a pupil's religion, or about managing a pupil's medical condition, don't name the child if you don't need to

### ✓ Think before you put information up on the wall

- If your display is an essential part of teaching and learning, or helps to keep pupils safe, it's fine. This might include medical information, or a list of parents' evening appointments. Still only display the information you really need to
- If your display is non-essential, promotional, or there might be a safeguarding risk, either ask the pupil or parents for consent first or just don't display it

### ✓ Take care when you're taking personal information home with you

- Sign documents containing personal data out and in from the school office

- Keep physical documents in a secure, closed folder along with your contact details in case the folder is lost
- Store the documents in a safe place at home – don't leave them in your car or at a friend's house

#### ✓ **Practise good ICT security**

- Passwords should be at least 8 characters, with upper and lower-case letters and special characters
- Password-protect documents and email attachments that include personal data
- Always double-check that you're emailing personal data to the correct person, who is authorised to see it
- Use 'bcc' when you're emailing a group of people who don't have email addresses for everyone else in the group, e.g. parents or volunteers

## **DON'T**

#### ✗ **Leave personal data out on your desk**

- Keep your desk clear, so people cannot see information about others accidentally. The same goes for personal data written on post-it notes, on top of the printer, or on an unattended computer screen

#### ✗ **Take any sensitive personal information home with you**

- If the information is confidential, sensitive or risky, it's best to leave it on the school site or computer system, where there are security measures and processes in place

#### ✗ **Use memory sticks**

- If you really need to use one, make sure it is encrypted

**If something doesn't seem right, talk to SBM data processor who will contact our data protection officer (DPO):**

. Claire Mehegan at [claire.mehegan@london.anglican.org](mailto:claire.mehegan@london.anglican.org)

**Report immediately if you think personal data has been lost, stolen or wrongly disclosed. This is so we can quickly take steps to mitigate the impact of the breach.**

You should also speak out if:

- You have any concerns at all about keeping personal data safe
- You're introducing a new process or policy that involves using personal data
- Anyone asks you to see the data that we have about them – this is called a 'subject access request' and our DPO will need to deal with this