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 number, attendance and assessment information, financial information, email address

Sensitive personal data (or special category data): includes genetic data; biometric data; data that **reveals** someone's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; and data **concerning** someone's health, sex life or sexual orientation

DO

✔ Remember that data protection laws DO NOT stop you from sharing information in order to keep children safe

- You must still share this information with the relevant people if it's to help keep a child safe. 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 unless you 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 their 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 back 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, numbers 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 already all have each other's email addresses, e.g. parents or volunteers

DON'T

✖ Leave personal data out on your desk

- Keep your desk clear, so people can't see information about others accidentally. The same goes for personal data written on sticky 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's encrypted

If something doesn't seem right, talk to our data protection officer (DPO):

The Onto Group – 0161 504 6921 / GDPR@theontogroup.com

Report to our DPO 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 to our DPO 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 if they can see the data that we have about them – this is called a 'subject access request' and our DPO will need to deal with this