SaintGREGORY'S
Bath

Data Protection Guidelines

Title	Data Protection Guidelines		
Prepared By	Karen Tyler, Data Manager	Date:	May 2018
Last Checked By	Clare Murray, IT Governor	Date:	September 2022
Last Approved By	Governors' Finance and Premises Committee	Date:	September 2023
Version	V01.05		
Document Update	September 2024		

Version	Date	Amendments
V01.00	September 2018	Approved by Governors
V01.01	May 2019	Information regarding logins for visitors
V01.02	September 2020	Changed who provides logons for visitors
V01.03	September 2021	Added guidance regarding whiteboards
V01.04	September 2022	Added guidance about posting data and reporting breaches
V01.05	September 2023	Reapproved by Governors

"In Christ we flourish"

Data Protection Guidelines

All staff must be particularly mindful of the requirement to keep personal data secure. You will routinely create and access personal data in your role, (e.g. every time you look at information about a pupil’s attainment or needs, or whenever you make a note regarding a pupil’s ability or mark their work). You must therefore follow these guidelines in relation to any personal data you process:

- Papers containing personal data should be kept in a locked filing cabinet, drawer or safe when not in use. Personal data should **never** be put on tables or desks that students work at.
- Papers containing personal data should not be left unattended or in clear view in any shared areas.
- Heads of Year offices and faculty offices should be locked when a member of staff is not present if any confidential records are there which are not locked away.
- Students should not enter Heads of Year offices, faculty offices or student support offices unless all personal data has been put out of sight.
- Where personal data is taken off the premises, (whether electronic or paper format), staff will take extra care to follow the same procedures for security whilst it is off site. The person taking the information is responsible for its security whist it is off site.
- All papers containing personal data should either be shredded or placed in Confidential Waste sacks for disposal. Confidential Waste sacks should be looked after. They should be kept in a locked office or filing cabinet whilst being filled. Once full, please ask a member of the site team to collect it or take it to the main office. Never leave Confidential Waste sacks unattended in corridors whilst waiting for them to be collected.
- When papers containing personal data are to be posted or handed to a parent/carer, student or a person outside of the school community, care must be taken to ensure that only data the recipient is entitled to see is included. Staff should ask a colleague to check what is being placed in the envelope.
- If data is kept electronically it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up.
- All electronic devices should be password protected to protect the information on the device in case of theft. Passwords should be “strong”, i.e. contain a mixture of upper and lower case letters, digits and punctuation marks.
- If data needs to be kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer or safe and if possible encrypted.
- Memory sticks should not be used for personal information. If you are given a memory stick with data on, please encrypt it immediately.
- If staff use their mobile phones to access school emails, they must be careful to make sure no-one else is able to see their phone when doing so. Their phone must be password protected and have suitable security software on it.
- All members of staff who need access to the school network are provided with their own secure login and password. Staff must not use another person’s login and must not pass their login details to anyone else. Staff will be prompted to change their password every 90 days.

- All visitors requiring access to the school network must be given a visitor login and password. Please ask the Data Manager or the Cover Manager to provide these.
- Staff must take care to ensure that personal data (including assessment results and registers and other information from SIMS or Class Charts) is not displayed on the whiteboard in their classroom.
- All classroom staff must log off their computer when leaving the room.
- Emails containing sensitive or confidential information are to be password-protected if there are unsecure servers between the sender and the recipient.
- When sending emails that include personal data, care must to taken to check the email address/recipient information is correct before sending. Attachments must also be checked before sending.
- When you receive an email containing personal data, save the data on your "Home" drive and then permanently delete the email. Remember to retain the personal data for only as long as you need it.
- Circular emails to parents or other contacts are to be sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- Before sharing data, all staff members will ensure that they are allowed to share the data, including making sure that this use of the data has been outlined in the appropriate Privacy Notice. If at all unsure, they should check with the DPO first, unless it is a medical emergency or an immediate Child Protection issue.
- Great care must be taken to ensure that visitors do not access personal information inappropriately.
- All potential data breaches must be reported immediately to the Data Protection Officer, Mrs Karen Tyler. In her absence, they should be reported to the Facilities and ICT Manager, Mr Gerry Cross or the Business Manager, Mr Adam Sheldon.