Saint GREGORY'S Bath

Data Protection Policy

Key Information

Title	Data Protection Policy	
Prepared By	Karen Tyler, Data Manager	May 2018
Checked By	Lisa Slater, Data Governor	June 2018
Approved By	Governors	11 September 2018
Version	V01.00	
Document Update	May 2019	

Version History

Version	Date	Amendments
V01.00	11 September 2018	Approved by Governors

"In Christ we flourish"

Introduction

St Gregory's Catholic College (the school) is a Data Controller for the purposes of Data Protection law and must comply with Data Protection legislation. This policy is intended to ensure compliance and in particular to make sure that all staff and governors are aware of their responsibilities in terms of Data Protection. The School has appointed the Data Manager, Mrs Karen Tyler, as its Data Protection Officer (DPO). Any questions about this policy should be sent to her.

Status of this Policy

This policy does not form part of the contract of employment of staff but it is a condition of employment that employees will abide by school policies and procedures. Any failures to follow the policy could therefore result in disciplinary action.

Background

The school needs to collect and use certain personal information about its staff, students, parents/carers and other individuals who come into contact with us. We need to process 'personal data' for a variety of reasons, such as to recruit and pay our staff, to record the academic progress of our students and to comply with statutory obligations (for example, health and safety requirements and our reporting obligations to central government and to the Local Authority).

To comply with the law, all personal data that is processed by us must be collected and used fairly, stored safely and must not be disclosed to any third persons unlawfully.

What data is covered by the Law and by this Policy?

Personal Data is very widely defined. It includes any personal information at all from which a living individual can be identified. It therefore includes such things as people's names, addresses, email addresses, contact details, staff records, student data, photographs, video recordings and expressions of opinion about individuals.

Sensitive Personal Data is also referred to in the legislation as 'special categories of personal data', and includes information that shows people's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual orientation, and health and genetic data or biometric data. Special rules apply whenever sensitive data is used.

All such data used for school business is covered, whether it is held in paper files or electronically. It doesn't matter where the data is held. It covers data held on school premises or on a PC at someone's home and it includes data held on mobile devices (such as on electronic notebooks or laptops) and regardless of who owns the device on which it is stored.

Basic Principles

To ensure compliance with the legislation the school must comply with the Data Protection Principles. In summary, these state that all personal data held shall be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- Accurate and, where necessary, kept up-to-date;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Commitment

The school is committed to complying with the data protection principles and the law. Therefore we will:

- Publish comprehensive, clear privacy notices for staff, students, parents/carers and other student contacts, so that they understand what information of theirs and their child's we hold, why it is held and who it may be shared with;
- Ensure that this policy is reviewed and updated from time to time so that it reflects best practice for everyone to follow;
- Ensure that all staff and governors are aware of and understand this policy and related procedures;
- Provide training and support on data protection to ensure best practice;
- Implement appropriate technical and organisational measures to ensure that personal data held by or on behalf of the school is kept safe and secure and protect all such personal data from loss, theft and unauthorised access or disclosure;
- Ensure that only authorised persons have access to personal data processed by the school;
- Check the accuracy of the information we hold at regular intervals;
- Ensure that personal data is not retained for any longer than necessary and unrequired data is deleted or destroyed as soon as practicable. Paper documents will be shredded or placed in Confidential Waste sacks. Electronic memories will be scrubbed clean or destroyed. Please see our Data Retention Policy for information about how long data will be kept for.
- Share personal data with third parties only when it is legally appropriate to do so.
- Comply with the legal duty to respond to subject access requests within the specified time limits.
- Ensure that personal data is not transferred outside of the EEA without appropriate safeguards.

To assist with this we shall keep records of our main internal processing activities and monitor these activities. Our records will include the following information:

- What personal data is being processed
- The purposes of the processing
- Where the data will be stored
- How long the data will be kept for
- Who the data will be shared with
- A description of the technical and organisational security measures.

Data Protection Officer (DPO)

The DPO is responsible for informing and advising the school and its staff about their obligations to comply with data protection laws.

Monitoring the school's compliance will include managing internal data protection activities, advising on Data Protection Impact Assessments, conducting internal audits, and providing training to staff members.

The DPO will report to the Headteacher. They will operate independently and will not be dismissed or penalised for performing their task. Sufficient resources will be provided to the DPO to enable them to meet their legal obligations.

However, compliance with Data Protection law is the responsibility of all members of St Gregory's and everyone has their role to play.

General Responsibilities of Staff and Governors

- When appointed, staff and governors must consent to their personal data being processed.
- They must also ensure that any personal information that they provide to the school in connection with their role is accurate and up to date and notify the school as soon as possible of any changes to it.
- They are responsible for ensuring that they adhere to data protection legislation in the course of carrying out their role, and must seek advice if they are ever unsure.
- If they discover a potential or actual breach of security and/or of data protection they must advise the DPO immediately. See 'Data Breaches' below.
- They must be mindful of the need for confidentially and not disclose personal data to third parties unless they have firstly obtained the consent of the individual concerned or the disclosure is made due to a statutory obligation (e.g. in the case of safeguarding). This means that personal data must not be disclosed either verbally or in writing or via web pages or by any other means, accidentally or otherwise, to any unauthorised third party.
- They must take particular steps to ensure that any personal data that they hold is kept securely so that it cannot be accessed by third parties. Particular care must be taken when transferring data (eg via email). Personal data should not be held or transferred onto mobile devices unless absolutely necessary and appropriate security measures are in place. You must use passwords and you may need to use encryption when transferring data. See "Specific Duties regarding Data Security for Staff" below for more information.

Specific Duties regarding Data Security for Staff

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

These guidelines are published separately in a document called "Data Protection Guidelines".

Responsibilities of Parents/Carers and Students

All parents/carers are responsible for:

- Checking that any information that they provide to the school in connection with their child/themselves is accurate and up to date.
- Informing the school of any changes to information that they have provided, e.g. change of address, as soon as possible.

Use of Personal Data relating to Students

When parents/carers provide personal data to us (such as details pertaining to their child's health or educational needs) they will be giving us permission to process that data for all subsequent purposes relating to their child's schooling or education. This means that the information could be used for a number of purposes, from considering special educational needs provision, to matters relating to discipline.

CCTV and Photography

We notify students and staff that we use CCTV and the reasons for this in our Privacy Notices and visitors are notified on arrival. Cameras are only placed where they do not intrude on anyone's privacy and where they are necessary to fulfil their purpose.

All CCTV footage will normally be kept for 30 days for security purposes. The Site Manager is responsible for keeping the records secure and allowing access to them.

The school will always indicate its intentions for taking photographs of students and will obtain permission (from the parents or the students themselves if they are in the sixth form) before publishing them. Images captured by individuals for their own recreational/personal purposes, and videos made by parents for family use, are exempt from data protection law.

Data Breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The DPO will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the school is legally obliged to report the breach to the regulatory authority (the ICO) within 72 hours of the school becoming aware of the breach. If a breach is not reported in time the school could risk an additional fine. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis. If a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will normally also notify those concerned directly.

If a member of staff becomes aware of a breach, they must report this immediately to the DPO. In her absence, it should be reported to the Director of Business and Finance, Mrs Karen Howard. The Data Manager will investigate the breach and write a "Breach Notification" report.

The Breach Notification will normally include the following:

- The nature of the personal data breach, including the categories of data and the approximate number of individuals and records concerned.
- An explanation of the likely consequences of the personal data breach.
- A description of the proposed measures to be taken to deal with the personal data breach.
- A description of the measures taken to mitigate any possible adverse effects.