Trinity School

Data Protection Policy and GDPR

DOCUMENT REVIEW
GOVERNOR APPROVAL DATE: 9 March 2018
COMMITTEE RESPONSIBLE: Resources Committee
NEXT REVIEW DATE: 1 March 2019

Table of Contents

Data Protection Policy

Introduction

Purpose:

This document is a statement of the aims and principles of the School, for ensuring the confidentiality of sensitive information relating to staff, pupils, parents and governors.
Trinity School needs to keep certain information about its employees, students and others to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, Trinity School must comply with the Data Protection Principles which are set out in the GDPR.

Aim(s):

To comply with the Data Protection Act, we will ensure that personal data will:

- be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- be adequate, relevant and not excessive for that purpose.
- be accurate and kept up to date.
- not be kept for longer than is necessary for that purpose.
- be processed in accordance with the data subject's rights.
- be kept safe from unauthorised access, accidental loss or destruction.

Consultation

Governors
All governors were provided with draft copies of the document for review and comment.

Sources and references:

Data Protection; The Principles. Information Commissioner
http://www.ico.gov.uk/for_organisations/data_protection/the_guide/the_principles.aspx
Report on the Data Protection Guidance we gave schools in 2012, Information Commissioner

Procedures and practice

The Data Controller and the Designated Data Controllers

The School as a body corporate is the Data Controller under the GDPR, and the Governors are therefore ultimately responsible for implementation. However, the Designated Data Controllers will deal with day-to-day matters.

The School has two Designated Data Controllers:

Mr B Williams is the Data Protection Lead within the School.

Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the appropriate Designated Data Controller, who would be:

Either Mr B Williams (Data Protection Lead)
bwilliams@trinitysevenoaks.com

Or the Data Protection Officer (who maintains an impartial position) at dpo@trinitysevenoaks.com

The Data Audit
An annual audit is to be approved by the Data Controller and the Governors of the School. The audit must record all types and sources of personal data kept by the School as well as the grounds for keeping the data, the extent to which the data is used and the measures that are being taken to keep the data secure.

Staff training
It is the responsibility of the Data Protection Lead to ensure staff members are trained in the management of personal information.

Responsibilities of Staff
All staff members are responsible for:

- Checking that any information that they provide to the School in connection with their employment is accurate and up-to-date.
- Informing the School of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The School cannot be held responsible for any errors unless the staff member has informed the School of such changes.
- If and when, as part of their responsibilities, staff members collect information about other people (e.g. about a student's course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff set out in the Schools Data Protection Code of Practice. (Appendix A)
- Information that is found to be out-of-date must be brought to the attention of the Data Controller and updated.

Data Security
All staff members are responsible for ensuring that:

- Any personal data that they hold is kept securely.
- Active steps are taken to avoid personal information being seen by students/adults without a clear reason.
- Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.
- Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.
- Computers are screen-locked when unattended.
- Paper documents containing sensitive information must be kept securely.

Personal information should:

- Only be collected or processed if necessary and can be identified as meeting one of the legal justifications.

- Be kept in a locked filing cabinet, drawer, or safe; or
- If it is computerised, **be held only on school-issued computers** where it will be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up; and
- **Should not be kept on a diskette or other removable storage media**, without permission from the Data Controller in which case that media must itself be kept in a locked filing cabinet, drawer, or safe.

Restricted access
All personal information is to be used and kept strictly out of necessity. Personal data should be kept to a minimum in general.

Data Privacy Impact Assessments
When new data is recorded, a DPIA must be conducted with the new data added to the audit.

Rights to Access Information "Data Subject Access Request"

All staff, parents and others whose data is held are entitled to:

- Know what information the School holds and processes about them or their child and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what the School is doing to comply with its obligations under the GDPR.

This Policy document and the School's Data Protection Code of Practice address in particular the last three points above. To address the first point, the School will, upon request, provide all staff and parents and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the School holds and processes about them, and the reasons for which they are processed.

All staff, parents and others have a right under the GDPR to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should put this request in writing to the Designated Data Controller.

The School will not charge to access data unless there is a significant cost to the School in terms of time or resources.

The School aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 30 days, as required by the GDPR.

Subject Consent

In many cases, the School can only process personal data with the consent of the individual.

In some cases, if the data is sensitive, as defined in the GDPR, express consent must be obtained. Agreement to the School processing some specified classes of personal data is a condition of acceptance of employment for staff.

This includes information about previous criminal convictions. Employment with the School will bring the applicants into contact with children. The School has a duty under the Children Act

1989 and other enactments to ensure that staff members are suitable for the job. The School has a duty of care to all staff members and students, and must therefore make sure that employees and those who use School facilities do not pose a threat or danger to other users.

The School may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes. The School will only use this information in the protection of the health and safety of the individual, but will need consent to process this data in the event of a medical emergency, for example.

Processing and Storing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, or race. This may be to ensure that the School is a safe place for everyone, or to operate other School policies, such as the Sick Pay Policy or the Equal Opportunities Policy. Because this information is considered **sensitive** under the GDPR, staff (and students where appropriate) will be asked to give their express consent for the School to process this data. An offer of employment may be withdrawn if an individual refuses to consent to this without good reason.

Particular care must be taken when storing sensitive information. IT systems (SIMS and network files) must be maintained to allow password protected access to designated staff, those who need to process information (SLT broadly, pastoral leaders). Safeguarding information is stored under lock and key with only the DSL and a deputy able to freely access the information.

If this information is needed for reasons other than originally obtained, specific permission must be sought. Sensitive information may be kept separately from other information on a particular individual to ensure that it is only used as initially intended.

Occasions of sharing sensitive information should be very rare. Any electronic communication should be encrypted/password protected to ensure there is no data breach.

Publication of School Information

Certain items of information relating to School staff will be made available via searchable directories on the public website, in order to meet the legitimate needs of researchers, visitors and enquirers seeking to make contact with the School.

Data collection

All personal data collected must specify its purpose for collection and any other purpose for its intended use. It must also specify who will be able to access the data.

Retention of Data

The School has a duty to retain some staff member and student personal data for a period of time following their departure from the School, mainly for legal reasons, but also for other purposes such as being able to provide references or academic transcripts. Different categories of data will be retained for different periods of time.

Outdated data will be removed from the school system (SIMS has a facility to delete data) or paper records destroyed by shredding.

Privacy Notices

The School will make publically available 3 privacy notices instructing individuals of their rights and the data held on them.

1. Student information notice (aimed at parents)
2. Student information notice (simpler language and aimed at children)
3. Staff workforce

Concluding notes

Compliance with the GDPR is the responsibility of all members of the School. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or even to a criminal prosecution.

Registration

Data Controller Name: Trinity Sevenoaks School Limited
Registration Number: Z3276436
Security Number: 10966073

Complaints

Complaints regarding the application of this policy should be made to the Chairperson of the Governing Board who will decide if it is appropriate for the complaint to be dealt with under the complaints procedure. Complaints which are not dealt with under the School's complaint procedure should be forwarded in writing to the Information Commissioner. It is likely that complaints about procedural issues, due process and timeliness will be dealt with by the Governing Board. Complaints that involve consideration of personal data or sensitive personal data should be referred to the Information Commissioner through the data protection officer.

Contacts

If you have any concerns or questions in relation to this policy, please contact the School's data controllers who will also act as the contact point for any requests under the Data Protection Act.

Further advice and information, including a full list of exemptions, is available from the Information Commission, www.informationcommissioner.gov.uk 01625 545 700.

Monitoring and review:

This policy will be reviewed annually to ensure compliance with relevant legislation.

Other documents and appendices:

Appendix A: What is Personal Data – A quick reference Guide (Information Commissioner)
Appendix B: Use of Images
Also see Access to Students Records Policy

Appendix A: What is Personal Data?

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive personal data

The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9).
The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).

Appendix B: Use of Images

- Parents, legal guardians, family members and friends can take images of their child and friends participating in School's activities for family and personal use.
- Parents will be asked for their permission before photography is allowed.
- Before they are allowed to take images during School's activities, parents or legal guardians have to sign an agreement that any images they take will not be used inappropriately.
- Parents or family members wishing to take images during an activity will be asked to sign a dated register.
- Photography and video filming will be limited to designated areas.
- Use of cameras and other equipment will be monitored.

Images for School's publications:

- The School will only take and use images that are appropriate and are considered to not be open to misuse.
- If an image of a child is used, the child's name will not be published. If a name is published, no image will be used without specific consent.
- Children will be made aware of why their picture is being taken and how it will be used.
- Children will be given the option to not have their image used if they are the sole focus of the picture.
- Children and parents should be encouraged to recognise the value of group photographs or recordings of School's events.
- Images will be kept securely and held by the School for the duration of the pupil's time there, after which they will be destroyed.
- Images of children from the School will not be used to illustrate controversial subjects.

Images for the School's website:

The School's websites are part of the internet and are more easily accessible than paper based School's publications. The School will make sure that only appropriate images are used. Image filenames will avoid using children's names.

Webcams:

- Webcams are a useful tool for learning. They can allow an individual or class to interact over the internet with others and support links between pupils in different schools, countries and cultures.
- A webcam will only be used in appropriate circumstances such as a normal class setting.
- Both children and teachers will be made aware of when a webcam is in use.

CCTV:

The School uses CCTV in some areas of School's property as a security measure.
Cameras will only be used in appropriate areas and there will be/is clear signage indicating where it is in operation.