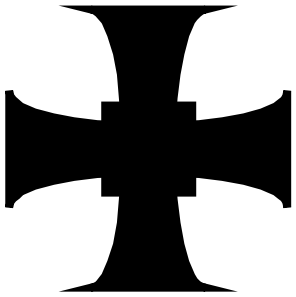
TRINITY SCHOOL
CARLISLE



A CHURCH OF ENGLAND ACADEMY

GDPR POLICY
(GENERAL DATA PROTECTION REGULATION)

Full Governing Body
Reviewed: September 2018
Ratified by the full Governing Body: September 2018
Next review: September 2019

Introduction

Background to the General Data Protection Regulation ('GDPR')

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

Aim

The aim of this policy is to ensure that Trinity School implements the new elements of data protection associated with the General Data Protection Regulation (GDPR) and associated Data Protection Bill which will replace the current Data Protection Act 1998.

Trinity School is committed to protecting the rights and privacy of individuals – students and staff and others, in accordance with the General Data Protection Regulation.

Purposes

Like all schools, Trinity School needs to have and to use certain information about its staff, students and other individuals with whom it has a relationship for various purposes. These include:

- the recruitment and payment of staff, and matters relating to their employment;
- the administration of the school's curriculum, and timetable;
- the monitoring and reporting of students' progress, including attendance and other pastoral information which allows us to enact our duty of care for students;
- monitoring behaviour and rewarding students;
- organising education visits, including residentials;
- collecting fees for examinations and trips etc.;
- fulfilling our legal obligations to funding bodies and to government departments, to other agencies outside the school.

There may be other purposes beyond this list for which the school will have the need to have and to use information about students and staff and other individuals.

Trinity School will seek to ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully. We will seek to comply with various legal obligations, including the obligations imposed on it by the General Data Protection Regulations

.

Associated School Policies

- Overarching Safeguarding Statement
- Child Protection Policy
- E-Safety Policy and Acceptable Use Agreements
- CCTV Procedures
- Health and Safety Policy
- Procedures for Using Students' Images
- Whole School Behaviour Policy

Compliance

Policy statement

1.1 The Co-Headteachers, Senior Leadership Team and Governing Body, located at Trinity School are committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information Trinity School collects and processes in accordance with the General Data Protection Regulation (GDPR).

1.2 The GDPR and this policy apply to all of Trinity School personal data processing functions, including those performed on customers', clients', employees', suppliers' and partners' personal data, and any other personal data the organisation processes from any source.

1.3 Data Protection Officer is responsible for reviewing the register of processing annually in the light of any changes to Trinity School activities to any additional requirements identified by means of data protection impact assessments. This register needs to be available on the supervisory authority's request.

1.4 This policy applies to all Employees/Staff and interested parties of Trinity School such as outsourced suppliers. Any breach of the GDPR will be dealt with under Trinity School disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

1.5 Partners and any third parties working with or for Trinity School, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by Trinity School without having first entered into a **data confidentiality agreement**, which imposes on the third party obligations no less onerous than those to which Trinity School is committed, and which gives Trinity School the right to audit compliance with the agreement.

This policy applies to all staff and students of Trinity School. Any breach of this policy, or of the Act itself, will be considered an offence and the school's disciplinary procedures could be invoked.

We expect other agencies who work with us to have their own General Data Protection Regulation policy and to work with us on the basis of compliance with the Act, with their own policy and with ours. The various departments in the school who are responsible for dealing with external agencies will take responsibility for ensuring that such agencies work with us in this way to protect individuals' data.

The Information Commissioner's Office (ICO) https://ico.org.uk/ gives further detailed guidance and Trinity School undertakes to adopt and comply with ICO guidance.

Trinity School may be required to share personal information about its students or staff with other schools, organisations, the LA and social services.

This policy applies to computerised systems and manual records, where personal information is accessible by specific criteria, chronologically or as pseudonymised data, e.g. key-coded. It also applies to photographs, CCTV footage and audio and video systems.

LEGAL FRAMEWORK

This policy has due regard to legislation, including, but not limited to the following:

- General Data Protection Regulation (GDPR)
- Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)

- Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

This policy also has regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

Definitions used by Trinity School (drawn from the GDPR)

Material scope (Article 2) – the GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

Territorial scope (Article 3) – the GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behavior of data subjects who are resident in the EU.

Article 4 definitions

Establishment - the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use,

disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behavior. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child – the GDPR defines a child as anyone under the age of 16 years old, (although this may be lowered to 13 by Member State law. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

2. Responsibilities and roles under the General Data Protection Regulation

Trinity School is a data controller under the GDPR. The Co-Headteachers, Senior Leadership, Governing Body and all those in managerial or supervisory roles throughout Trinity School are responsible for developing and encouraging good information handling practices within Trinity School responsibilities are set out in individual job descriptions.

2.1 The Data Protection Officer (DPO), a role specified in the GDPR, should be a member of the senior management team and have appropriate authority, is accountable to the Co-Headtachers, Senior Leadership Team and Governing Body of Trinity School for the management of personal data within the School and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

2.1.1 development and implementation of the GDPR as required by this policy; and
2.1.2 security and risk management in relation to compliance with the policy.

The Data Protection Officer for Trinity School is Mr A Winter, Assistant Headteacher – Sixth Form

2.2 A Data Protection Officer, who the Co-Headteachers consider to be suitably qualified and experienced, has been appointed to take responsibility for Trinity School compliance with

this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that Trinity School complies with the GDPR, as do the Senior Leadership team in respect of data processing that takes place within their area of responsibility.

2.3 The Data Protection Officer has specific responsibilities in respect of procedures such as the Subject Access Request Procedure (see Appendix A) and is the first point of call for Employees/Staff seeking clarification on any aspect of data protection compliance.

2.4 Compliance with data protection legislation is the responsibility of all Employees/Staff of Trinity School who process personal data.

2.5 Trinity School's Training Policy sets out specific training and awareness requirements in relation to specific roles and Employees/Staff of Trinity School generally.

2.6 Employees/Staff of Trinity School are responsible for ensuring that any personal data about them and supplied by them to Trinity School is accurate and up-to-date.

3. Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. Trinity School's policies and procedures are designed to ensure compliance with the principles.

3.1 Personal data must be processed lawfully, fairly and transparently

Lawful – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent.

Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

The GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' requirement.

Transparently – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

Trinity School's Privacy Notice is recorded in a separate document (see Appendix C)

The specific information that must be provided to the data subject must, as a minimum, include:

3.1.1 the identity and the contact details of the controller and, if any, of the controller's representative;

3.1.2 the contact details of the Data Protection Officer;

3.1.3 the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

3.1.4 the period for which the personal data will be stored;

3.1.5 the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;

3.1.6 the categories of personal data concerned;

3.1.7 the recipients or categories of recipients of the personal data, where applicable;

3.1.8 where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;

3.1.9 any further information necessary to guarantee fair processing.

3.2 Personal data can only be collected for specific, explicit and legitimate purposes

Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of Trinity School's GDPR register of processing and as explained in the Privacy Procedure

3.3 Personal data must be adequate, relevant and limited to what is necessary for processing

3.3.1 The Data Protection Officer is responsible for ensuring that Trinity School does not collect information that is not strictly necessary for the purpose for which it is obtained.

3.3.2 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be include a fair processing statement or link to privacy statement and approved by the Data Protection Officer

3.3.3 The Data Protection Officer will ensure that, on an as appropriate basis all data collection methods are reviewed by internal audit/external auditors to ensure that collected data continues to be adequate, relevant and not excessive.

3.4 Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

3.4.1 Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

3.4.2 The Data Protection Officer is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

3.4.3 It is also the responsibility of the data subject to ensure that data held by Trinity School is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

3.4.4 Employees/Staff/parents/students should be required to notify Trinity School of any changes in circumstance to enable personal records for updating records are contained. It is the responsibility of Trinity School to ensure that any notification regarding change of circumstances is recorded and acted upon.

3.4.5 The Data Protection Officer is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

3.4.6 On at least an annual basis, the Data Protection Officer will review the retention dates of all the personal data processed by Trinity School, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed.

3.4.7 The Data Protection Officer is responsible for responding to requests for rectification from data subjects within one month (Subject Access Request Procedure). This can be extended to a further two months for complex requests. If Trinity School decides not to comply with the request, the Data Protection Officer must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

3.4.8 The Data Protection Officer is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

3.5 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

3.5.1 Where personal data is retained beyond the processing date, it will be minimised/encrypted/pseudonymised in order to protect the identity of the data subject in the event of a data breach.

3.5.2 The Data Protection Officer must specifically approve any data retention that exceeds the retention periods identified in the requirements of the data protection legislation. This approval must be written.

3.6 Personal data must be processed in a manner that ensures the appropriate security

The Data Protection Officer will carry out a risk assessment taking into account all the circumstances of Trinity School's controlling or processing operations.

In determining appropriateness, the Data Protection Officer should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on Trinity School itself, and any likely reputational damage including the possible loss of customer trust.

When assessing appropriate technical measures, the Data Protection Officer may consider the following:

- Password protection;
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media;
- Virus checking software and firewalls;
- Role-based access rights including those assigned to temporary staff;
- Encryption of devices that leave the organisations premises such as laptops;
- Security of local and wide area networks;
- Privacy enhancing technologies such as pseudonymisation and anonymisation;

When assessing appropriate organisational measures the Data Protection Officer will consider the following:

- The appropriate training levels throughout Trinity School;
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper based records;
- Adoption of a clear desk policy;
- Storing of paper based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Manage the use of employee's own personal devices being used in the workplace through technical solutions/BYOD policy;
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

3.7 The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

Trinity School will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans.

4. Data subjects' rights

4.1 Data subjects have the following rights regarding data processing, and the data that is recorded about them:

- 4.1.1 To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- 4.1.2 To prevent processing likely to cause damage or distress.
- 4.1.3 To prevent processing for purposes of direct marketing.
- 4.1.4 To be informed about the mechanics of automated decision-taking process that will significantly affect them.
- 4.1.5 To not have significant decisions that will affect them taken solely by automated process.
- 4.1.6 To sue for compensation if they suffer damage by any contravention of the GDPR.
- 4.1.7 To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.
- 4.1.8 To request the supervisory authority to assess whether any provision of the GDPR has been contravened.
- 4.1.9 To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
- 4.1.10 To object to any automated profiling that is occurring without consent.

Trinity School ensures that data subjects may exercise these rights:

- 4.1.11 Data subjects may make data access requests as described in Subject Access Request Procedure ; this procedure also describes how Trinity School will ensure that its response to the data access request complies with the requirements of the GDPR.
- 4.1.12 Data subjects have the right to complain to Trinity School related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the Complaints

5. Consent

5.1 Trinity School understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of

personal data relating to him or her. The data subject can withdraw their consent at any time.

5.2 Trinity School understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

5.3 There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. The Controller must be able to demonstrate that consent was obtained for the processing operation and record kept of this.

5.4 For sensitive data, explicit written consent of data subjects must be obtained following the School's consent procedure unless an alternative legitimate basis for processing exists.

5.5 In most instances, consent to process personal and sensitive data is obtained routinely by Trinity School using standard consent documents. e.g. when a new client signs a contract, or during induction for participants on programmes.

5.6 Where Trinity School provides online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 16.

6. Security of data

6.1 All Employees/Staff are responsible for ensuring that any personal data that Trinity School holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Trinity School to receive that information and has entered into a confidentiality agreement.

6.2 All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy. All personal data should be treated with the highest security and must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected in line with DfE/Ofsted guidelines in the Access Control Policy and/or
- stored on (removable) computer media which are encrypted in line with Secure Disposal of Storage Media.

6.3 Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees/Staff. All Employees/Staff are required to enter into an Acceptable Use Agreement before they are given access to organisational information of any sort, which details rules on screen time-outs.

6.4 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit written authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving in line with the Trinity School data retention guidelines.

- Personal data may only be deleted or disposed of in line with the Retention of Records Procedure as 'confidential waste'.
- Hard drives of redundant PCs are to be removed and immediately destroyed or as disposed of in line with Secure Disposal of Storage Media

6.5 Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

7. Disclosure of data

7.1 Trinity School must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain

circumstances, the Police. All Employees/Staff should exercise caution when asked to disclose personal data held on another individual to a third party. Staff should seek advice from the Data Protection Officer if there is any concern

7.2 All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer

8. Retention and disposal of data

8.1 Trinity School shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

8.2 Trinity School may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

8.3 The retention period for each category of personal data will be set out in the Retention of Records Procedure) along with the criteria used to determine this period including any statutory obligations Trinity School has to retain the data.

8.4 Trinity School data retention and data disposal procedures will apply in all cases.

8.5 Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects. Any disposal of data will be done in accordance with the secure disposal procedure

9. Data transfers

9.1 All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

The transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply:

9.1.1 An adequacy decision such Privacy Shield or Assessment of adequacy has been undertaken

A list of countries that currently satisfy the adequacy requirements of the Commission are published in the *Official Journal of the European Union.* *http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm*

9.1.2 The existence of Binding corporate rules or Model contract clauses

10. Information asset register/data inventory

10.1 Trinity School has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance project. Trinity School data inventory and data flow determines

- business processes that use personal data;
- source of personal data;
- volume of data subjects;

- description of each item of personal data;
- processing activity;
- maintains the inventory of data categories of personal data processed;
- documents the purpose(s) for which each category of personal data is used;
- recipients, and potential recipients, of the personal data;
- the role of the Organisation Name throughout the data flow;
- key systems and repositories;
- any data transfers; and
- all retention and disposal requirements.

10.2 Trinity School is aware of any risks associated with the processing of particular types of personal data and makes the appropriate assessment such as DPIA.

Document Owner and Approval

The Data Protection Officer / GDPR Owner is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

A current version of this document is available to all members of staff on the [location]**.**

This policy was approved by the xxxx on [date] and is issued on a version controlled basis.

Signature: Date:

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	Xxxx	Xxxx

Appendix A **Subject Access Request Procedure**

Trinity School

1. Scope

All personal data processed by Trinity School is within the scope of this procedure.

Data subjects are entitled to obtain:

- Confirmation as to whether the school is processing any personal data about that individual;
- Access to their personal data;
- Any related information;
- The logic involved in any automated decisions relating to him or her.

2. Responsibilities

1.1 The Data Protection Officer is responsible for the application and effective working of this procedure, and for reporting to the Co-Headteachers and Governing Body on Subject Access Requests (SARs).

1.2 The Data Protection Officer is responsible for handling all SARs.

Procedure

3.1 Subject Access Requests are made/recorded using the Subject Access Request Form.

3.2 The data subject provides the School with evidence of their identity, in the form of a current passport/driving license, Birth Certificate, recent utility bill, bank statement or current Vehicle Registration Document, and the signature on the identity must be cross-checked to that on the application form

3.3 The data subject specifies to Trinity School specific set of data held by Trinity School on their subject access request (SAR). The data subject can request all data held on them.

3.4 The School records the date that the identification checks were conducted and the specification of the data sought.

3.5 The School provides the requested information to the data subject within one month from this recorded date. There are no circumstances in which an extension to that one month will be provided, and failure to provide the requested information within that one month is a breach of the GDPR.

3.6 Once received, the subject access request (SAR) application is immediately forwarded to the Data Protection Officer, who will ensure that the requested data is collected within the specified time frame in clause 3.4 above.
Collection entails:

3.6.1 Collecting the data specified by the data subject, or

3.6.2 Searching all databases and all relevant filing systems (manual files) in Trinity School, including all back up and archived files (computerised or manual) and all email folders and archives.

3.6.3 Data may not be altered or destroyed in order to avoid disclosure.

3.7 The Data Protection Officer maintains a record of requests for data and of its receipt, including dates.

3.8 The Data Protection Officer / GDPR Owner reviews subject access requests from a child. Before responding to a SAR of the child data subject the Data Protection Officer / GDPR Owner considers their ability to making the request.

3.9 The Data Protection Officer / GDPR Owner reviews all documents that have been provided to identify whether any third parties are present in it, and either removes the identifying third party information from the documentation or obtains written consent from the third party for their identity to be revealed.

3.10 If any of the requested data is being held or processed under one of the following exemptions, it does not have to be provided:

- National security
- Crime and taxation
- Health
- Educational records or relates to social work
- Regulatory activity
- Journalism, literature and art
- Research history, and statistics
- Publicly available information
- Corporate finance
- Examination marks
- Examinations scripts
- Domestic processing
- Confidential references
- Judicial appointments, honours and dignities
- Crown of ministerial appointments
- Management forecasts
- Negotiations
- Legal advice and proceedings
- Self-incrimination
- Human fertilization and embryology
- Adoption records
- Special educational needs
- Parental records and reports

3.11 In the event that a data subject requests the School to provide them with the personal data stored by the controller/processor, then the School will provide the data subject with the requested information in electronic format, unless otherwise specified. All of the items provided to the data subject are recorded on a schedule that shows the data subject's name and the date on which the information is delivered to, and received by, the data subject.

3.12 In the event that a data subject requests what personal data is being processed then the School provides the data subject with the following information:

3.12.1 Purpose of the processing

3.12.2 Categories of personal data

3.12.3 Recipient(s) of the information, including recipients in third countries or international organisations

3.12.4 How long the personal data will be stored

3.12.5 The data subject's right to request rectification or erasure, restriction or objection, relative to their personal data being processed.

3.12.5.1 The School removes personal data from systems and processing operations as soon as a request for erasure has been submitted by the data subject.

3.12.5.2 The School contacts and communicates with other organisations, where the personal data of the data subject is being processed, to cease processing information at the request of the data subject.

3.12.5.3 The School takes appropriate measures without undue delay in the event that the data subject has: withdrawn consent; objects to the processing of their personal data in whole or part; no longer under legal obligation and/or has been unlawfully processed.

3.12.6 Inform the data subject of their right to lodge a complaint with the supervisory authority and a method to do so.

3.12.7 Information on the source of the personal data if it hasn't been collected from the data subject.

3.12.8 Inform the data subject of any automated decision-making.

3.12.9 If and where personal data has been transferred and information on any safeguards in place.

Document Owner and Approval

The Data Protection Officer is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the GDPR.

This procedure was approved by the xxx on date and is issued on a version controlled basis under his/her signature.

Signature: Date:

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	xxx	xxx

Appendix B **Subject Access Request Form**

Trinity School

---

1. Data Subject Details:

Title	Mr ☐	Mrs ☐	Miss ☐	Ms ☐	Other: ☐
Surname					
First name(s)					
Current address					
Telephone number:					
Home					
Work					
Mobile					
Email address					
Date of birth					
Details of identification provided to confirm name of data subject:					
Details of data requested:					

1.1 **Details Of Person Requesting The Information** (if not the data subject):

Are you acting on behalf of the data subject with their *[written]* or other legal authority?	Yes ☐ No ☐				
If 'Yes' please state your relationship with the data subject (e.g. parent, legal guardian or solicitor)					
Please enclose proof that you are legally authorised to obtain this information.					
Title	Mr ☐	Mrs ☐	Miss ☐	Ms ☐	Other: ☐
Surname					
First name(s)					
Current address					

Telephone number:	
Home	
Work	
Mobile	
Email address	

2. Declaration

I, ……, the undersigned and the person identified in (1) above, hereby request that Trinity School provide me with the data about me identified above.

Signature: Date:

SAR form completed by (employee name):

I, ……, the undersigned and the person identified in (1.1) above, hereby request that Trinity School provide me with the data about the data subject identified in (1) above.

Signature: Date:

SAR form completed by (employee name):

This form must immediately be forwarded to Trinity School's Data Protection Officer.

Appendix C : **Trinity School Privacy Notice**

Trinity School

Privacy Notice (How we use student information)

Introduction
This notice is to help you understand how and why we collect personal information about you and what we do with that information.

What is personal information?
Personal information is information that identifies you as an individual and relates to you. This includes your contact details, next of kin and financial information. We may also hold information such as your religion or ethnic group. CCTV, photos and video recordings of you are also personal information.

The categories of student information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address, CCTV photos and video recordings)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information (such as targets, data collections, reports, test and examination results)
- Relevant medical information (such as medication details, allergies, medical conditions and notes from meetings/GPs/other health care professionals)
- Special Education Needs information (such as Education and Health Care Plans (EHCPs), Individual Education Plans (IEPs) and notes from review meetings and professional assessments)
- Behaviour information (such as behaviour logs, achievement points, exclusions)
- Safeguarding information
- Biometric data (measurements from fingerprint)
- Post 16 learning information and destination data

Why we collect and use this information

We use the student data:

- to support student learning
- to monitor and report on student progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing
- to provide appropriate careers advice and guidance
- to ensure students are safe
- to monitor attendance
- to contact next of kin in case of emergency
- to enable access to catering facilities
- to celebrate students' achievements

The lawful basis on which we use this information

We collect and use personal data in order to meet legal requirements and legitimate interests set out in the General Data Protection Regulation (GDPR) and UK law, including those in relation to the following:

- Article 6 and Article 9 of the GDPR
- Education Act 1996
- Regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013

Please see the following website for more information: **https://www.gov.uk/education/data-collection-and-censuses-for-schools**

Collecting student information

Whilst the majority of student information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain student information to us or if you have a choice in this.

Storing student data

Personal data relating to students is stored in line with the school's GDPR Policy. In accordance with the GDPR, the school does not store personal data indefinitely; data is only stored for as long as is necessary to complete the task for which it was originally collected.

Who we share student information with

We routinely share student information with:

- Schools, colleges and universities that students attend after leaving us
- Employers when requesting references
- Cumbria Local Authority and Children's Services (this includes Social Services, the SEND team and Targeted Youth Support), under strict information sharing protocols and policies. We may be required to share this information with other public sector partners such as other Local Authorities or local Children Centres
- Department for Education (DfE)
- Examination boards
- Police
- NHS (this includes Child and Adolescent Mental Health Service)
- Pupil Referral Unit (this includes Hospital and Home Tuition Service)
- INSPIRA
- Third Party organisations that subject areas use to support student learning e.g Mathswatch

Why we share student information

We do not share information about our students with anyone without consent unless the law and our policies allow us to do so.

We share student's data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.
We are required to share information about our students with the (DfE) under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Youth support services

Students aged 13+

Once our students reach the age of 13, we also pass student information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996. This enables them to provide services as follows:

- youth support services
- careers advisers

A parent or guardian can request that **only** their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child /student once he/she reaches the age 16.

Students aged 16+

We will also share certain information about students aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996. This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

For more information about services for young people, please visit our local authority website.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.
We are required by law, to provide information about our students to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.
To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.
The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.
For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data
For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, parents and students have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact **Mr A Winter, Assistant Headteacher & Data Protection Officer, email dataprotection@trinity.cumbria.sch.uk**

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact:
Mr A Winter, Assistant Headteacher & Data Protection Officer,
email dataprotection@trinity.cumbria.sch.uk

Appendix D Student Acceptable Use Agreement Form

The computer system is owned by the school. This Responsible Use policy helps to protect students, staff and the school by clearly stating what use of the computer resources is acceptable and what is not. This is a summary of the full school Acceptable Use policy.

- Irresponsible use will result in the loss of computer access to all school ICT resources.
- Network access must be made via the user's authorised account and password, which must not be given to another person. You will be responsible for any computer activity done on your password.
- School computer and internet use must be appropriate to your education.
- Copyright and intellectual property rights must be respected.
- E mail should be written carefully and politely, particularly as messages may be forwarded or printed to be seen by unexpected readers.
- Users are fully responsible for e mail they send and for contacts made.
- Personal contact information (e.g. phone numbers and addresses) must not be typed into web pages or e mail.
- Anonymous messages and chain letters are not permitted.
- The use of chat rooms and messaging services is not allowed.
- You are not allowed to download any programs or games from the internet. If in doubt you should check with the ICT Services Manager in Creighton building.
- The use of proxy sites is expressly forbidden.
- The school ICT systems including printers may not be used for personal purposes.
- The ICT system and system security must be respected
- No food or drink should be brought near any of the ICT resources

The school will exercise its right to monitor the use of the school computer systems, including access to web sites, the interception of e mail, and the deletion of inappropriate materials where it believes unauthorised use of the school system is or may be taking place.

I agree to abide by the conditions of the ICT Responsible Use Policy and understand the implications if I do not.

Signed _____ Date _____