TRINITY SCHOOL
CARLISLE

A CHURCH OF ENGLAND ACADEMY

Data Protection Policy

Full Governing Body
Reviewed: February 2022
Ratified by the full Governing Body: March 2022
Next review: February 2023

1. Aims

Trinity School aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed under the UK GDPR and the Data Protection Act (2018).

2. Scope

The School is a 'Data Controller' for the purposes of processing personal data. This means that the School determines the purpose and means of the processing of personal data.

This policy applies to current and former employees, governors, volunteers, apprentices and any other stakeholders who work for or on behalf of the School If you fall into one of these categories, then you are a 'data subject' for the purposes of this policy. Please read this policy alongside your contract of employment (or contract for services) and any other notice the School issues from time to time relating to your personal data.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

The School has ***Privacy Notices*** in place relating to the processing of personal data related to governors, staff, job applicants, students, parents and other categories of data subjects. Copies can be obtained from the Office or are available for staff on the N drive under school policies.

The School has measures in place to protect the security of personal data in accordance with its ***Data Security Policy*** and the ***Data Classification and Handling Procedure***.

The School will only hold data for as long as necessary for the purposes for which it was collected. Data will be retained and destroyed in accordance with the ***Data Retention Policy and Schedule***.

This policy explains how the School will hold and process personal data. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, the School

3. Legislation and Guidance

This policy meets the requirements of the UK GDPR and the Data Protection Act (2018). It is based on guidance published by the Information Commissioner's Office (ICO) on the Data Protection legislation and the ICO's code of practice for Subject Access Requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with our funding agreement and articles of association.

4. Definitions

The terms in this document have the meanings as set out in Article 4 of the UK GDPR unless amended by the Data Protection (Act 2018).

For clarity, the following have been reproduced:

> '**personal data**' means 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 category personal data**' means 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.
>
> '**processing**' means any operation or set of operations which is performed on personal data or 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.
>
> '**data controller**' means 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 processor**' means a person, other than an employee of the data controller, who processes the data on behalf of the data controller.
>
> '**data subject**' means a person whose personal data is held or processed.

5. The Data Controller

The School processes personal data relating to parents, students, staff, governors, visitors and others, and therefore is a data controller.

The School is registered as a data controller with the ICO – registration number Z2834725 and will renew this registration annually or as otherwise legally required.

The School delegates the responsibility of the Data Controller to the Data Controllers Representative (See Section 6 below).

6. Roles and Responsibilities

This policy applies to all staff employed by the School, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Governing Board

The governing board has overall responsibility for ensuring that the School complies with all relevant data protection obligations.

Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO will provide an annual report of their activities directly to the School Board and, where relevant, report to the board their advice and recommendations on school data protection issues.

DPO is also the first point of contact for individuals whose data the School processes, and for the ICO.

Our DPO is The Schools People (See Contact details below)

Principal

The Principal acts as the Data Controller's representation on a day-to-day basis.

All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the School of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - If they have any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
    - If there has been a data breach
    - Before engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

7. Data Protection Principles

The UK GDPR is based on data protection principles that the School must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes

- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

These six principles are further strengthened by the Accountability Principle which requires the School to demonstrate compliance with the UK GDPR.

This policy sets out how the School aims to comply with these principles.

8. Lawful Bases for Processing Personal Data

Lawfulness, Fairness and Transparency

We will only process general category personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the School can fulfil a contract with the individual, or the individual has asked the School to take specific steps before entering into a contract
- The data needs to be processed so that the School can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual e.g., to protect someone's life
- The data needs to be processed so that the School, as a public authority, can perform a task in the public interest, and carry out its official functions

Where the School is not operating in its capacity as a public authority, for example for the purposes of facilities hire, or after-School activities not tied to curriculum, the lawful basis for that processing will be legitimate interest.

The School may process personal data for these purposes without knowledge or consent.

The School will not use personal data for an unrelated purpose without disclosing the intent, providing the lawful basis for the processing and seeking consent if necessary.

Whenever personal data is collected from individuals, they will be provided with the relevant information including details of the data collected and how it is collected, stored and shared, via a Privacy Notice (sometimes called a Fair Processing Notice) as required by the UK GDPR and the Data Protection Act (2018).

When processing 'special categories' of personal data, the School will identify one of the special category conditions for processing set out in the UK GDPR (see below), and where relevant a condition specified in Schedule 1 to the Data Protection Act 2018 (see Appendix1:

Special Category Data

In processing 'special categories' of personal data, we comply with at least one of the special category conditions set out in the UK GDPR and Data Protection Act 2018, in that

- The data processed, ensures the vital interests of the individual where they are physically or legally incapable of giving consent
- The data has been made public by the individual e.g., on social media
- Processing is necessary to carry out rights and obligations under employment law
- Processing is necessary for the assessment of a person's working capacity either based on UK Law or under contract with a health professional such as an occupational health provider
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- Processing is necessary for reasons of substantial public interest, based on domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Consent

Where no other lawful basis for processing personal data exists, the School will seek consent from the Data Subject for that processing. For example, where the School wishes to use images of students or staff in marketing publications or on social media channels.

Consent must be informed, unambiguous and freely given. When relating to special category data the consent must also be explicit.

Where consent form is the only lawful basis for processing, that consent may be withdrawn at any time. The withdrawal of consent does not affect the lawfulness of the processing before the consent was withdrawn.

Criminal Convictions

The School may use information relating to criminal convictions where the law allows us to do so. The School may hold information about criminal convictions if information about criminal convictions comes to light as a result of our recruitment and Disclosure and Barring Service checks, or if any information about criminal convictions becomes apparent during a stakeholder's relationship with the Trust.

Information about criminal convictions and offences will be used in the following ways:

- To ensure employee suitability to work
- For safeguarding purposes.

Less commonly, information relating to criminal convictions may be used where necessary in relation to legal claims; where it is necessary to protect an individual's interests (or someone else's interests), and they are not capable of giving consent, or where information has already been made public.

9. Limitation, Minimisation and Accuracy

We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individual when we first collect their data through the provision of a Privacy Notice.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned and seek consent before we process this data.

Staff must only process personal data where it is necessary so that they can carry out their role effectively.

The School will take reasonable steps to ensure the accuracy of the data at the point of collection and during the data lifecycle.

When the School no longer need the personal data it holds, it will ensure it is stored, deleted or anonymised in accordance with the Schools ***Data Retention Policy and Schedule***.

10. Sharing Personal Data

The School is obliged to share personal data to meet obligations under contracts or to meet its statutory obligations. Examples of organisations with whom personal data may be shared regularly include, but are not limited to:

- Department for Education
- The Local Authority
- Ofsted
- Disclosure and Barring Service
- HMRC
- Teachers' Pension Service
- Local Government Pension Service

Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies, HR Consultants, Occupational Health Services, Wellbeing Services etc. When appointing such service providers, the School will:

- Only appoint suppliers or contractors who can provide sufficient guarantees that they comply with current data protection legislation
- Establish a data-sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carryout their service, and information necessary to keep them safe while working with us.

The School may also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided

Where necessary personal data may be shared with emergency services and local authorities to help them to respond to an emergency that affects any of our students or staff.

Other instances where personal data may be shared includes:

- Where an issue arises with a student or parent/carer that puts the safety of our staff at risk
- Where we need to liaise with other agencies – we will seek consent as necessary before doing this

11. Transferring Data Outside the UK

The School does not routinely share data with organisations outside the UK. Where this may be necessary, e.g., where a former employee has emigrated and/or applied to work outside the UK, data may be transferred to the new employer with explicit consent from the former employee and with appropriate safeguards.

Personal data will not be transferred outside the UK unless such transfer complies with the UK GDPR and the Data Protection Act (2018) where:

- The Secretary of State has decided that another country or international organisation ensures an adequate level of protection for personal data
- One of the derogations in the UK GDPR applies (including if an individual explicitly consents to the proposed transfer).

12. Data Security

Everyone who works for, or on behalf of, the Trust has responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Trust's Data Security and Data Retention policies.

Data Security - Organisational Measures

The School shall ensure that the following measures are taken concerning the collection, holding, and processing of personal data:

- All staff, volunteers, contractors, service providers or other parties working on behalf of the School shall be made fully aware of their individual responsibilities and the School's responsibilities under the UK GDPR and this Policy and shall have free access to a copy of this Policy

- Only those working for or on behalf of the School that require access to, and use of personal data to carry out their assigned duties shall have access to personal data held by the School
- Those working for or on behalf of the School who engage with the handling personal data will be appropriately trained to do so and adequately supervised
- Those working for or on behalf of the School shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise
- Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed
- All personal data held by the School shall be reviewed periodically, as set out in the School's Data Retention Policy.

Data Security -Technological Measures

The School shall ensure that the following measures are taken concerning IT and information security:

- The School requires that any passwords used to access personal data shall have a minimum of 8 characters, composed of a mixture of upper- and lower-case characters, numbers and symbols. Passwords are not expected to be changed regularly, but users will be expected to change their password when instructed by the School:
- Passwords should not be written down or shared between any staff or other parties working for or on behalf of the School, irrespective of seniority or function. If a password is forgotten, it must be reset using the applicable method.
- All software (including, but not limited to, applications and operating systems) shall be kept up to date. The School's IT staff shall be responsible for installing security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so; and
- No software may be installed on any School-owned computer or device without authorisation.

Contravention of these rules may be treated as a disciplinary matter.

Data Security - Storage

The School shall ensure that the following measures are taken concerning the storage of personal data:

- All electronic copies of personal data should be stored securely using passwords, user access rights and where appropriate data encryption
- All hard copies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar
- All personal data relating to the operations of the School, stored electronically, should be backed up regularly
- Where any member of staff stores personal data on a mobile device (whether that be a computer, tablet, phone or any other device) then that member of staff must abide by the School's ***Acceptable Use Policy***. The member of staff shall also ensure that they can provide a secure environment for that device to be used to minimise any risk to the confidentiality or integrity of the information.

Data Security – Disposal

The School shall ensure that the following measures are taken concerning the disposal of personal data:

- When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted or disposed of.
- The School may also use a third-party service provider to safely dispose of records. If we do so, we will require the third party to provide sufficient guarantees that it complies with current data protection law and provides a Certificate of Destruction for our records.

For further information on the deletion and disposal of personal data, please refer to the School's Data Retention Policy and Schedule

Data Security – Use of Personal data

The School shall ensure that the following measures are taken concerning the use of personal data:

- No personal data may be shared informally and if an employee, volunteer, processor, or other party working for or on behalf of the School requires access to any personal data that they do not already have access to. Such access should be formally requested from the relevant Business Manager.
- Personal data must always be handled with care and should not be left unattended or on view to unauthorised persons at any time
- If personal data is being viewed on a computer screen and the computer is to be left unattended, the user must lock the computer and screen before leaving it; and
- Where personal data held by the School is used for marketing purposes, appropriate checks to ensure consents for such processing are in place must be carried out before the data is used.

13. Data Breaches

The School has robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur then the School must record and keep evidence of that breach in perpetuity.

All personal data breaches must be reported immediately to the internal data protection lead and/or the Data Protection Officer.

If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure the Information Commissioner's Office is informed of the breach without delay, and within 72 hours after having become aware of it.

If a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

Data breach notifications shall include, as a minimum, the following information:

- The categories and approximate number of data subjects concerned

- The categories and approximate number of personal data records concerned
- The name and contact details of the Trust's data protection officer (or another contact point where more information can be obtained)
- The likely consequences of the breach.
- Details of the measures taken or proposed to be taken, by the Trust to address the breach including, where appropriate, measures to mitigate possible adverse effects.

For further information please refer to the ***Data Security Policy and Breach Procedure***.

14. Subject Access Requests and Other Data Subject Rights

Subject Access Requests (SARs)

Data subjects may make subject access requests ("SARs") at any time to access the personal data that the School holds about them. Data subjects are encouraged to approach the School directly to make a request.

Staff wishing to make a SAR may approach their line manager, the DPO, or submit it directly to the School.

The School must respond within one month unless the request is complex or numerous, in which case the response can be extended by a further two months. If such additional time is required, the data subject shall be informed without undue delay.

Responses to SARs shall be dependent upon the terms of the UK GDPR, the Data Protection Act (2018) and associated ICO guidance.

There is no fee for making a SAR. However, if a request is deemed manifestly unfounded or excessive the School may charge a reasonable administrative fee or refuse to respond to the request

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

The School has defined a process for handling SARs and other data subject requests.

All SARS will be recorded together with any requests that have been refused.

For further information please refer to the ***Subject Access Request Policy and Procedure***

Other Data Protection Rights of the Individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to the processing at any time if consent is the sole basis for processing
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)

- Prevent the use of their personal data for direct marketing
- Challenge processing which has been justified based on public interest
- Request a copy of agreements under which their personal data is transferred outside of the UK (if relevant)
- Object to decisions based solely on automated decision making or profiling (if relevant)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights directly to the School.

15. Parental Requests to Education Records

The parental right of access to the educational record is only relevant to maintained schools. Parents/carers of a child under 12 years of age, may request access to the educational record via a Subject Access Request.

Requests to access the educational record of a student 12 years of age or older must be accompanied by a third-party consent signed by the student.

16. CCTV

We use CCTV in various locations in and around the School site. We will adhere to the ICO's code of practice for the use of CCTV.

The purpose of the system is to prevent crime and promote security and public safety. If, in the event of viewing CCTV for the specified purpose a disciplinary action is observed, the CCTV can and may be used to support a disciplinary or criminal investigation.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

For more information about the School's use of CCTV please refer to ***CCTV Policy.***

Any enquiries about the CCTV system should be directed to the IT Services Manager.

17. Photographs and Videos

As part of School activities, we may take photographs and record images of individuals within the School

With the exception of photographs required for identification purposes, staff must not take images of students unless they have:

- a legitimate reason for doing so
- parental consent to do so. Please be aware that parental consent may be overridden by the student at any time

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain to the parent/carer and student how the photographs and/or video will be used. Uses may include:

- Within the School on notice boards and in School magazines, brochures, newsletters, etc.
- Outside of the School by external agencies such as the School photographer, newspapers, campaigns
- Online on our School website or social media pages

When using photographs and videos in this way we will not accompany them with any other personal information about the student, to ensure they cannot be identified.

Consent may be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

18. Biometric Data Processing

The School uses Biometric Data to manage pupil access to services including catering, entry/exit points and printing.

A student under 18 years of age cannot lawfully consent to the processing of their personal data

Biometric Data must not be taken from a student under 18 years of age without explicit, written consent from at least one parent/carer

Consent provided by one parent may be overridden by the written objection of another parent

Consent provided by one or more parents/carers may be overridden by an objection (either verbal or non-verbal), or a refusal to co-operate with the process, by a student.

19. Accountability & Record Keeping

The Schools Data Protection Officer is The Schools People, who can be contacted by emailing DPOService@schoolspeople.co.uk or calling 01773 851 078

The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for

monitoring compliance with this Policy, the School's other data protection-related policies, and compliance with the UK GDPR and other applicable data protection legislation.

The School shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

- The name and details of the School, its Data Protection Officer, and any applicable third-party data processors
- The purposes for which the School collects holds, and processes personal data:
- Details of the categories of personal data collected, held and processed by the School, and the categories of data subject to which that personal data relates
- Details of any transfers of personal data outside the UK, including all mechanisms and security safeguards
- Details of how long personal data will be retained by the School (please refer to the School's Data Retention Policy & Schedule); and
- Detailed descriptions of all technical and organisational measures taken by the School to ensure the security of personal data.

20. Data Protection by Design and Default

The School will put measures in place to demonstrate that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 7)
- Completing Data Protection Impact Assessments where the School's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this and any related policies, and any other data protection matters. Records of staff training events and attendance will be maintained.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our School and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)

For all personal data that we hold, we will maintain an internal Record of Processing Activities, including the categories of data processed, the categories of Data Subject, the purpose of the processing, third-party recipients, how the data is stored, retention periods and how we are keeping the data secure.

21. Data Protection Impact Assessments

The Trust shall carry out Data Protection Impact Assessments for all new projects and/or new uses of personal data which involve the use of new technologies/new service providers and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the UK GDPR.
Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

- The type(s) of personal data that will be collected, held and processed
- The purpose(s) for which personal data is to be used
- The Trust's objectives
- How personal data is to be used
- The parties (internal and/or external) who are to be consulted
- The necessity and proportionality of the data processing related to the purpose(s) for which it is being processed
- Risks posed to data subjects
- Risks posed both within and to the Trust; and
- Proposed measures to minimise and handle identified risks.

22. Personal Data Breaches

The School will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in our ***Data Security Policy and Breach Procedure***.
When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches may include, but are not limited to:

- A non-anonymised dataset being published on the School website showing the exam results of students eligible for the pupil premium
- safeguarding information being made available to an unauthorised person
- theft of a School laptop containing non-encrypted personal data about students.

23. Training

All staff and governors are provided with data protection training as part of their induction process. Data protection training will also form part of continuing professional development programme.

Additional training will be provided in response to changes in the data protection legislation, patterns of personal data breaches are identified, or changes to the School's processing activities make it necessary.

24. Monitoring Arrangements

The Data Controller's Representative together with the Data Protection Officer are responsible for monitoring and reviewing this policy.

The Data Controller's Representative, together with the Data Protection Officer check that the School complies with this policy by, among other things, reviewing records, policies and procedures annually.

This policy will be reviewed and updated as and when necessary following any amendments to Data Protection legislation or guidance, or any internal concerns resulting from policy violations, data breaches, or on an annual basis.

At every review, the policy will be shared with the Governing Board.

Effective From:	May 2018
Last Update:	February 2022
Next Review Date:	February 2023

25. Contacts

Questions or concerns about how the School processes personal data or any requests to exercise data protection rights, should be submitted to the School in the first instance.

If the School is not able to address concerns and resolve them satisfactorily, please contact the Data Protection Officer at the address below.

Finally, concerns can be registered with the UK's data protection regulator, the Information Commissioner's Office, by following this link https://ico.org.uk/make-a-complaint/

Contact Details

Data Controller: Trinity School, Strand Road, Carlisle, CA1 1JB.

Data Controller's Representative: Andrew Winter - Assistant Headteacher
Email: awi@trinity.cumbria.sch.uk

Data Protection Officer: Dee Whitmore.
Email: dposervice@schoolspeople.co.uk
Telephone: 01773 851 078;
Postal Address: The Schools People
44 Tyndall Court
Peterborough
Cambridgeshire
PE2 6LR.

26. Links to other policies and documents:

- Data Retention Policy and Schedule
- CCTV Policy

Appendix 1: Appropriate Policy Document

For use when relying on specified conditions for the processing of special categories of personal data, and personal data relating to criminal convictions and offences

1. Introduction

This is the 'Appropriate Policy Document' required when Trinity School seeks to rely on any of the conditions specified in Schedule 1 to the Data Protection Act 2018, for the processing of special category and criminal convictions personal data.

The content of this Appropriate Policy Document meets the requirements of paragraph 39 of Schedule 1 of the Data Protection Act (2018), in that it –

- explains the School's procedures for securing compliance with the principles in Article 5 of the UK General Data Protection Regulation ('UK GDPR') - principles relating to the processing of personal data, in connection with the processing of personal data in reliance on the condition in question; and
- explains the School's policies as regards the retention and erasure of personal data processed in reliance on the condition, indicating how long such personal data is likely to be retained.

Under paragraph 40(1) of Schedule 1 of the DPA (2018), where the School processes personal data in reliance on a condition described in paragraph 38 of Schedule 1, they will, during the relevant period[1]

- retain the appropriate policy document,
- review and (if appropriate) update it from time to time, and
- make it available to the Information Commissioner, on request, without charge

2. Description of Data Processes

As part of its statutory and business functions, the School processes special category data related to stakeholders, including staff, governors and volunteers, job applicants, pupils and parents/carers. This includes where relevant, information about health, disability and wellbeing, ethnicity, trade union membership, religious or philosophical beliefs, biometric data. Further information about this processing can be found in the relevant Privacy Notices.

Processing for reasons of substantial public interest relates to the data the School receives, obtains, or creates to fulfil our statutory obligations. For example, this may be related to the safeguarding of pupils, supporting staff with a particular disability or medical condition, for equal opportunities monitoring, safeguarding, etc.

A record of our processing activities is kept under Article 30 of the UK GDPR.

[1] The 'relevant period' begins when the data is collected and ends no less than 6 months following cessation of the processing

3. Schedule 1 Condition for Processing

The School processes special category data for the following purposes in Part 1 of Schedule 1 of the Data Protection Act (2018):

- Paragraph 1: Employment, social security and social protection.

The School may process special category data for the following purposes in Part 2 of Schedule 1 of the Data Protection Act (2018):

- Paragraph 6: Statutory, etc. purposes.
- Paragraph 8: Equality of opportunity and treatment.
- Paragraph 16: Support for individuals with a particular disability or medical condition
- Paragraph 17: Counselling
- Paragraph 18: Safeguarding of children and individuals at risk
- Paragraph 20: Insurance
- Paragraph 21: Occupational Pensions

4. Criminal Offence Data

The School processes criminal offence data for the following purposes in parts 1 and 2 of Schedule 1 of the Data Protection Act (2018).

- Paragraph 1 – employment, social security and social protection
- Paragraph 6(2)(a) – statutory, etc. purposes
- Paragraph 18 (1) Safeguarding of Children and individuals at risk

5. Securing Compliance with the Data Protection Principles

The School's procedures for complying with Article 5 of the GDPR: Data Protection Principles are as follows:

Principle A: Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

The School will:

- ensure that personal data is only processed where at least one of the conditions in Schedule 1 is met or the data subject has given their explicit consent for the processing.
- only process personal data fairly and will ensure that data subjects are not misled about the purposes of any processing.
- ensure that data subjects receive full privacy information so that any processing of personal data is transparent (provision of privacy notices).
- where necessary carry out Data Protection Impact Assessments to ensure proposed processing is carried out fairly.

Principle B: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
The School will:

- only collect personal data for specified, explicit and legitimate purposes and will inform data subjects what those purposes are through the provision of privacy notices.
- not use personal data for purposes that are incompatible with the purposes for which it was collected.
- before personal data is used for a new purpose that is compatible, the School will inform the data subject.

Principle C: Personal data shall be adequate, relevant and limited to what is necessary for the purposes for which they are processed.
The School will:

- only collect the minimum personal data needed for the purpose for which it is collected.
- ensure the data is adequate and relevant to the purpose for which it is collected.
- apply Data Protection Impact Assessments to ensure proposed processing is not excessive.
- Where personal data is provided to, or obtained by the School but is not relevant to a stated purpose, it will be erased.

Principle D: Personal data shall be accurate and, where necessary, kept up to date.
The School will ensure that:

- personal data is accurate and kept up to date as necessary.
- when notified of inaccuracies personal data is corrected.
- Where the School become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, every reasonable step will be taken to ensure that data is erased or rectified without delay. If the School decides not to either erase or rectify it, for example, because the lawful basis relied upon to process the data means these rights don't apply, the decision not to erase will be documented.

Principle E: Personal data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
The School will ensure that:

- personal data will only be kept in identifiable form only as long as is necessary for the purposes for which it is collected unless otherwise required by law.
- when no longer needed, personal data shall be securely deleted or anonymised.
- personal data is held and disposed of in line with the School's Data Retention Policy and Schedule.

Principle F: Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures.
The School will ensure that:

- there are appropriate organisational and technical measures in place to protect personal data.
- data is processed in accordance with its Data Handling and Classification Procedure and Data Security Policy and Procedure.

6. Accountability Principle

Under GDPR Article 5(2), the School is responsible for and must be able to demonstrate compliance with the principles listed above.
The School has appointed a Data Protection Officer in accordance with Article 37 of the UK GDPR. The DPO provides independent advice and monitoring of personal data handling and has access to report to the highest management level.
The School will:

- ensure that records are kept of all personal data processing activities and that these are provided to the Information Commissioner on request (RoPA).
- carry out a Data Protection Impact Assessment for any high-risk personal data processing and consult the Information Commissioner if appropriate.
- have in place internal policies and procedures to ensure that personal data is collected, used or handled only in a way that is compliant with data protection law.
- Policies for Retention and Erasure of Personal Data
- The School will ensure, where special category or criminal convictions personal data is processed, that:
- there is a Record of Processing Activities (ROPA), and that record will set out, where possible, the envisaged time limits for erasure of the different categories of data.
- where special category or criminal convictions personal data is no longer required for the purpose for which it was collected, it will be securely deleted or rendered permanently anonymous in accordance with the School's Data Retention Policy and Schedule.
- data subjects receive a Privacy Notice (sometimes called a fair processing notice) detailing how their data will be handled, including the period for which the personal data will be stored, or, if that is not possible, the criteria used to determine that period.

7. Additional Special Category Processing

The School processes special category personal data in other instances where there is not a requirement to keep an Appropriate Policy Document. Our processing of such data is in accordance with data protection legislation and respects the rights and freedoms of the data subjects.

The School will provide clear and transparent information about why personal data is processed including the lawful basis for processing in stakeholder Privacy Notices. Copies of Privacy Notices are available from the office.

8. Contact Information

If you have any questions or concerns about how the School process information or wish to exercise any data protection rights, please contact the School in the first instance.

If you have concerns that the School has not been able to resolve to your satisfaction you may contact the Data Protection Officer using the details below.

Alternatively, concerns can be registered the UK's data protection regulator, the Information Commissioner's Office by following this link https://ico.org.uk/make-a-complaint/

Contact Details

Data Controller: Trinity School, Strand Road, Carlisle, CA1 1JB.

Data Controller's Representative: Andrew Winter - Assistant Headteacher
Email: awi@trinity.cumbria.sch.uk

Data Protection Officer: Dee Whitmore.
Email: dposervice@schoolspeople.co.uk
Telephone: 01773 851 078;
Postal Address: The Schools People
44 Tyndall Court
Peterborough
Cambridgeshire
PE2 6LR.

Appendix 2: Review Updates

2022 - Revisions

Date	Revision
	Adoption of new policy