GDPR POLICY

Date: *July 2023*

Policy Review Cycle: *Annually*

Review Assigned to: *Trust Board*

Version Control

Version	Date	Changes	Approved
V1	May 2018	Implementation of GDPR	May 2018 by Trust
V2	June 2022	No significant change, clarification of wording and check to ensure compliant.	June 2022 by Trust
V3	July 2023	Content review and update	July 2023 by Trust

Introduction

The 1590 Trust processes personal data relating to students, visitors and others. This policy provides a framework for ensuring personal data is collected, stored and processed in accordance with the UK General Data Protection Regulations (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

Personal Data

Personal data the Trust may collect, use, store and/or share (where appropriate) includes but is not limited to:

- Contact details, contact preferences, date of birth, identification documents;
- Results of internal and external assessments;
- Curriculum records;
- Characteristics, such as ethnicity, eligibility for free school meals, special educational needs;
- Suspension information;
- Details of any medical conditions, (physical and/or mental);
- Attendance information;
- Safeguarding information;
- Details of any support received, including care packages, plans and support providers;
- Photographs and CCTV images captured in school;
- Biometric data (in conjunction with the Trust protection of biometric information policy).

Data protection principles

The following UK GDPR principles underpin the Trust's approach to processing personal data. In summary they require that personal data is:

1. Processed lawfully, fairly and in a transparent manner;
2. Used only for limited, specified stated purposes and not used or disclosed in anyway incompatible with those purposes;
3. Adequate, relevant, and limited to what is necessary;
4. Accurate and, where necessary, up to date;
5. Not kept for longer than necessary; and
6. Kept safe and secure.

In addition, the accountability principle provides protection for individuals when their personal data is being processed.

The majority of personal data is held and processed by the Trust as a public authority, to allow us to perform tasks in the public interest and carry out our official functions.

The Trust may collect and use personal data when there are grounds under the UK GDPR, including but not limited to the following:

- to fulfill a contract with an individual, or if an individual has asked the Trust to take specific steps before entering into a contract;
- To comply with a legal obligation;
- To ensure the vital interests of an individual e.g. to protect someone's life;
- To perform a task in the public interest and carry out official functions;
- For the legitimate interests of the Trust or a third party (provided an individual's rights

and freedoms are not overridden);

- An individual (or their parent/carer) has provided valid consent.

The Trust may process special categories of personal data in line with the special category conditions for processing set out in the GDPR and Data Protection Act 2018.

If the Trust offers online services to students such as classroom apps, consent will be obtained where necessary from students/parents/carers and in line with the GDPR and Data Protection Act 2018 (with the exception of online counselling and preventative services).

Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons and will endeavour to explain these reasons to the individuals upon collection.

If we need to use personal data for reasons other than those initially provided we will seek to inform the individuals concerned before we do so and seek consent where necessary.

Sharing personal data

The Trust will not generally share personal data but may do so where necessary for example if there is an issue with a student or parent/carer that puts the safety of our staff at risk, if we need to liaise with other public agencies or if our suppliers or contractors need data to enable us to provide services to our staff and students (for example IT companies. Necessary steps to protect the data will be taken by the Trust in line with the Data Protection Act 2018.

We will share personal data with law enforcement and government bodies where we are legally required to do so, for example for the prevention or detection of crime and/or fraud or where the disclosure is required to satisfy our safeguarding obligations.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff.

Information about students may be shared with third parties without consent if the law and our policies allow us to do so. Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about pupils with:

- The Local Authority to meet our legal obligations to share certain information with it, such as safeguarding concerns and suspensions;
- The Department for Education and Education and Skills Funding Agency;
- School aged Immunization Services providing vaccinations pursuant to The Health Service (Control of Patient Information) Regulations 2002;
- The student's family and/or representatives;
- Educators and examining bodies;
- Our regulator Ofsted;
- Suppliers and service providers to enable them to provide the service we have contracted them for;
- Our auditors;
- Police forces, courts, tribunals;
- Any other third party as required and in line with the Data Protection Act 2018.

National Pupil Database

We are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school census.

Some of this information is then stored in the National Pupil Database (NPD), which is owned and managed by the Department and provides evidence on school performance to inform

research.

The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data.

For more information, see the Department's webpage on how it collects and shares research data.

You can also contact the Department for Education with any further questions about the NPD.

Youth support services

Once our students reach the age of 13 we are legally required to pass on certain information about them to Stockton Council, as it has legal responsibilities regarding the education or training of 13-19 year-olds.

This information enables it to provide youth support services, post-16 education and training services and careers advisers.

Parents/carers, or students once aged 16 or above can contact our data protection officer to request that we only pass the individual's name, address and date of birth to Stockton Council.

Subject access requests

Individuals can make a 'subject access request' to gain access to their personal information held by the Trust. Subject access requests must be submitted for the attention of the Trust Data Protection Officer and should include details of the information requested.

Personal data about a child belongs to that child and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students may be granted without the express permission of the pupil. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our school may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

We may not disclose information for a variety of reasons, such as where it is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

Individuals should submit any request to exercise any of their rights under the Data Protection Act to the Trust Data Protection Officer preferably via dataprotection@1590trust.org.uk.

CCTV

We use CCTV in various locations around the Trust to ensure it remains safe. We do not need to request individuals' permission to use CCTV but aim to make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain prior, written consent from parents/carers for students for photographs and videos to be taken for communication, marketing and promotional materials. Where a student is 16 or over they are able to give their own consent.

Uses may include:

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

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will take appropriate action and update our records.

When using photographs and videos in this way we will not accompany them with any other personal information about the child.

Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

Access to sensitive data is restricted to approved users by the use of permissions and passwords.

Where we need to share personal data with a third party we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

Disposal of data

In the event personal data is no longer required the Trust will aim to dispose of the data securely. We may also use a third party to safely dispose of records on the Trust's behalf.

This policy can be read in conjunction with other policies such as the Trust Digital Data Security Policy and Trust school Child Protection Policies.

Monitoring arrangements

Trust Board
Headteacher
Data Protection Officer (DPO)
The Trust DPO is Natasha Healy and she is contactable via **dataprotection@1590trust.org.uk.**