



**TORQUAY BOYS' GRAMMAR SCHOOL  
MULTI ACADEMY TRUST**

**DATA PROTECTION  
POLICY**

# Data Protection Policy

## INTRODUCTION

The General Data Protection Regulation 2016 ( 'GDPR') aims to promote high standards in the handling of personal information protecting individuals' rights to privacy. The GDPR applies to anyone holding information about living individuals in electronic format and in some cases on paper. As Schools hold personal records they must also follow this Regulation.

The General Data Protection Regulation:

- Regulates the **processing** of personal data relating to **natural living persons** (data subjects)
- Imposes legal obligations upon **data controllers** (the Multi Academy Trust)
- Provides Data Subjects with legal rights relating to how their **personal data** is processed
- Introduces **sanctions** for breaches of the Regulation

## THE SIX PRINCIPLES OF THE GENERAL DATA PROTECTION REGULATION

- Principle 1:** Personal data must be processed fairly and lawfully and in a transparent manner.
- Principle 2:** Personal data must be processed for specific, explicit and legitimate purposes that are compatible with the original purpose of obtaining it.
- Principle 3:** Data collected and stored must be adequate, relevant and limited to what is necessary.
- Principle 4:** Data must be accurate and kept up-to-date.
- Principle 5:** Data must not be kept for longer than necessary.
- Principle 6:** Data must be processed in a manner which ensures appropriate security.

## SUMMARY

- Information about the Trust's Data Protection Policy is available from the Data Protection Officer and can also be viewed on either school's website.
- The Trust will give all data subjects the reasons for data collection, the purposes for which the data is held, the likely recipients of the data and the data subjects' right of access.
- All data subjects have a right of access to their own personal data. Such requests must be made in writing, using the Personal Data Subject Access Request form (available from the Data Protection Officer).
- The Trust will endeavour to ensure the accuracy of the data held.
- The data held will be accurate, relevant and not excessive.
- Staff must ensure that when staff or student information (electronic or otherwise) is taken off site that it is kept secure at all times.
- The Trust will ensure that all personal data held (be it in hard copy or electronic form) is secure.

The Multi Academy Trust has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.

The Headteacher and Governors of both Schools in the Trust intend to comply fully with the requirements and principles of the General Data Protection Regulation 2016 and the Data Protection Act 2018. All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.

## **WHO IS COVERED?**

The GDPR covers staff, students, parents and any other individuals for which either school holds personal details.

## **WHO IS RESPONSIBLE FOR ENSURING THAT THE SCHOOLS COMPLY WITH THE GDPR?**

Torquay Boys' Grammar School Multi Academy Trust will be the 'data controller' under the terms of the legislation – this means it is ultimately responsible for controlling the use and processing of the personal data. Torquay Academy and Torquay Boys' Grammar School will have controls in place to protect data at Academy level.

The Data Protection Officer has ultimate responsibility in ensuring that the schools comply with this act on a day to day basis, however, everyone within each school has a responsibility to ensure that they abide by the principles listed above in handling personal data. If you are unsure about the action you are taking with regard to personal data, you must check with the Data Protection Officer to ensure you are complying with the GDPR and the DPA 2018.

Some of the questions you can ask yourself to ensure that the action you are taking will comply with the GDPR are:

- Do I really need this information about an individual? Do I know what I'm going to use it for?
- Do the people whose information I hold know that I've got it and are they likely to understand what it will be used for? Would any of them be surprised at what I'm doing with their personal information?
- If I'm asked to pass personal information on am I sure it's okay to do so under the GDPR? (check with the Data Protection Officer if unsure)
- Am I satisfied that the personal information I hold is secure be it on the computer or paper based?
- Is the personal data held accurate and up to date?
- Do I delete/destroy personal information (securely) as soon as I have no need for it?
- Is access to personal information limited only to those with a strict need to know? Who will have access to this information if I place it on computer file or hold on a paper record?

Ensure that any personal data that you hold is only shared with other members of school staff or authorities who are entitled to have access to this data. If you have any queries or concerns you must raise them with your line manager immediately, who can seek advice from the Data Protection Officer if necessary.

As an individual you also have a responsibility to ensure that the details held about you are accurate and kept up to date for example ensuring that the school is notified if you move house.

## **INDIVIDUAL RIGHTS**

All individuals (including staff) have a right under the GDPR to ask for a copy of the information held about them on computer and in manual filing systems.

Requests for access to personal data should be referred to the Data Protection Officer who will deal with it promptly and within a maximum of 15 school days from receiving the request.

The Schools will only monitor individual staff when there are concerns about the individual's use of e-mail, internet, telephone or other data that the member of staff may be using inappropriately. If monitoring is used for training purposes the individual will be made aware of this at the time.

## **ENQUIRIES**

Information about the Trust's Data Protection Policy is available from the Data Protection Officer and can also be viewed on either school's website. General information about the General Data Protection Regulation and the Data Protection Act 2018 can be obtained from the Information Commissioner's Office (ICO), ( [www.ico.org.uk](http://www.ico.org.uk) )

## **FAIR OBTAINING AND PROCESSING**

Torquay Boys' Grammar School Multi Academy Trust undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data is held, the likely recipients of the data and the data subjects' right of access. Information about the use of personal data is printed on the appropriate collection form. If details are given verbally, the person collecting will explain the issues before obtaining the information. Full information is included in the Trust's Privacy Notices, for both staff and students, available on each school website.

"*Data subject*" means an individual who is the subject of personal data or the person to whom the information relates.

"*Parent*" has the meaning given in the Education Act 1996, and includes any person having parental responsibility or care of a child.

## **DATA ACCURACY**

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs either School of a change of circumstances their computer (SIMS) record will be updated as soon as is practicable.

Where a data subject challenges the accuracy of their data, the School will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the relevant Governing Body for their judgement. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

## **DATA ADEQUACY AND RELEVANCE**

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, both Schools will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

Annually, parents are asked to update the contact information held by each school for accuracy. Also, admin staff check any information held by each school against parental consent forms for trips.

## **LENGTH OF TIME**

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of staff to ensure that obsolete data is properly erased, using the Retention Schedule documentation available from the Data Protection Officer.

## **SUBJECT ACCESS**

The General Data Protection Regulation extends to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Where a request for subject access is received from a student, the Trust's policy is that:

- Requests from students will be processed as any subject access request as outlined below and the copy will be given directly to the student, unless it is clear that the student does not understand the nature of the request.

- Requests from students who do not appear to understand the nature of the request will be referred to their parents or carers.
- Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.

### **PROCESSING SUBJECT ACCESS REQUESTS**

Requests for access must be made in writing.

Students, parents or staff may ask for a Personal Data Subject Access Request form, also available from either School Website. Completed forms should be submitted to the Data Protection Officer. Provided that there is sufficient information to process the request, and that the identity of the requester has been verified, an entry will be made in the Subject Access Request Log, showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (e.g. Student Record, Personnel Record), and the planned date of supplying the information. Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be the date on which sufficient information has been provided.

In the case of any written request from a parent regarding their own child's record, access to the record will be provided within 15 school days in accordance with the current Education (Pupil Information) Regulations.

Access to CCTV Images are also covered by the Right of Access under the GDPR. A separate form is available for such requests, which is available from the Data Protection Officer. These requests will be subject to the same recording and processing as detailed above.

On receipt of the completed form, and subject to satisfactory identity verification, all Access Requests will be processed and completed by the relevant establishment before disclosure to the requester.

### **AUTHORISED DISCLOSURES**

The Trust will, in general, only disclose data about individuals with their consent. However, there are circumstances under which the Trust's authorised officers may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- Student data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations.
- Student data disclosed to authorised recipients in respect of their child's health, safety and welfare.
- Student data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of school.
- Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.
- Unavoidable disclosures, for example to an engineer during maintenance of the computer system or by any other Personnel. In such circumstances the engineer would be required to sign a non-disclosure form. Personnel working on behalf of the Academy or LA are contractually bound not to disclose personal data.
- Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within school by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the school who **need to know** the information in order to do their work. The school will not disclose anything on students' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything that suggests that they are, or have been, either the subject of, or at risk of, child abuse.
- The school must ensure that any 'third party' contractors, other than the LA, handling data sign an undertaking to abide by the principles of the General Data Protection Regulation.

A "**legal disclosure**" is the release of personal information from the computer to someone who requires the information to do his or her job within or for either school, provided that the purpose of that information has been registered.

An "**illegal disclosure**" is the release of information to someone who does not need it, or has no right to it, or one which falls outside either School's registered purposes. It is worth noting that comments on Facebook / Twitter etc. which disclose privileged personal data would fall into the category of 'illegal disclosure'.

## **DATA AND COMPUTER SECURITY**

Torquay Academy and Torquay Boys' Grammar School undertakes to ensure security of personal data in the following ways:

### **1) Physical Security**

Appropriate building security measures are in place, such as alarms, window bars, deadlocks and computer hardware cable locks. Only authorised persons are allowed in the computer rooms. Disks, tapes and printouts are locked away securely when not in use. Visitors to school are required to sign in and out, to wear identification badges whilst in school and are, where appropriate, accompanied.

### **2) Electronic Security**

Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files. Computer files are backed up (i.e. security copies are taken) regularly. Clearly, many documents in school contain sensitive and personal data (for example, IEPs, SEN statements and annual reviews, exclusion letters). Staff must ensure there is a specific requirement when taking a copy of these documents off-site. Memory sticks containing personal and sensitive data should be encrypted and documents password-protected. Technical assistance with this is available from the IT Department in either school.

### **3) Procedural Security**

- In order to be given authorised access to the computer, staff will have to undergo checks and will agree an acceptable use policy.
- Staff should not leave their computers logged on to personal data (for example, SIMS) when they are not present in the room.
- All staff are trained in their Data Protection obligations and their knowledge updated as necessary.
- Computer printouts as well as source documents containing personal data are shredded before disposal. (For example, personal data recorded for school trips)
- Students' school record files should not be taken off-site except under exceptional circumstances
- Staff should avoid leaving documents containing personal and sensitive data in places easily seen by others; for example, left on desks at the end of the day.

Overall, the security policy for data is determined by each Governing Body and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent.

Individual members of staff can be personally liable in law under the terms of the Data Protection Act 2018 and the General Data Protection Regulation. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

## MISCELLANEOUS

CCTV within school will only be in public areas, will not intrude on anyone's privacy and be used for security purposes. Notices will be placed in school to ensure that all visitors and staff are aware of this.

The Trust will also ensure that any service providers used that will handle personal data for example HR or Payroll comply with the GDPR.

Any member of staff found to mishandle data or share personal data with unauthorised individuals will be subject to investigation under the school's Disciplinary Policy. Deliberate, malicious or reckless breaking of the GDPR will be counted as gross misconduct and could result in dismissal. Under this Regulation you can also be criminally liable if you knowingly or recklessly disclose personal information in breach of the policy.

If there are any queries concerning this policy or you require further assistance or training, please contact the Data Protection Officer.

Further details on any aspect of this policy and its implementation can be obtained from the school.

Further advice and information on data protection can be obtained from the Information Commissioner's Office, [www.ico.gov.uk](http://www.ico.gov.uk).

Guidance: <http://www.ictknowledgebase.org.uk/dataprotectionpolicies>  
[http://www.ico.gov.uk/for\\_organisations/data\\_protection/the\\_guide.aspx](http://www.ico.gov.uk/for_organisations/data_protection/the_guide.aspx)


PTO for Data Subject Declaration>>>



## Personal Data Subject Access Request

(General Data Protection Regulation – Articles 15 to 22)

Under the Data Protection Act 2018, you have a right to access data relevant to you. If you wish to access data about someone else then you shall require their written consent, which you must make available to us. You may be committing an offence to seek data about other individuals without their consent.

Please complete this form and return to: **DATA PROTECTION OFFICER, Torquay Boys' Grammar School, Shiphay Manor Drive, Torquay Devon TQ2 7EL**

### 1. Personal Details - we may make additional checks to verify your identity.

Name:			
Present Address:			
		Post Code:	
Telephone number:		Date of Birth:	

### 2. The Data you wish to Access

Are you the subject of the access request?	Yes / No
Do you have Parental Responsibility for a student who is the subject of the access request?	Yes / No
If yes, please provide the name of the student(s) about whom you are making the access request	

Please specify the relevant data you are requesting access to:

### 3. Declaration

Declaration:  
 I request that you provide me with a copy of the personal data about me (or a student for which I have Parental Responsibility) which you hold and I have indicated above.  
 I confirm that I am the Data Subject (or Parent of) and am not acting on behalf of someone else.

Signed:	Date:

## CCTV Data Subject Access Request (General Data Protection Regulation – Articles 15 to 22)

Under the Data Protection Act 2018, you have a right to access data relevant to you. If you wish to access data about someone else then you shall require their written consent, which you must make available to us. You may be committing an offence to seek data about other individuals without their consent.

Please complete this form and return to: **DATA PROTECTION OFFICER, Torquay Boys' Grammar School, Shiphay Manor Drive, Torquay Devon TQ2 7EL**

### 1. Personal Details - we may make additional checks to verify your identity.

Name:			
Present Address:			
	Post Code:		
Telephone number:		Date of Birth:	

### 2. CCTV Details

Please note that unless this section is completed and a passport sized photograph of yourself is attached, then no search of data will be made.

Date to be viewed:		Specific Time: Start	
Where was the camera?		Specific Time: Finish	

Describe what you expect to see:

**PLEASE NOTE: CCTV Data is only held for 28 days**

### 4. Declaration

Declaration:

I request that you provide me with a copy of the personal data about me (or a student for which I have Parental Responsibility) which you hold and I have indicated above.

I confirm that I am the Data Subject (or Parent of) and am not acting on behalf of someone else.

Signed:	Date:
---------	-------

## Subject Access Request Template Letter

I understand that you wish to exercise your rights under the Data Protection Act 2018 to;

*[Please set out which right you are exercising]*

The Multi Academy Trust is obliged under the Data Protection Act 2018 to satisfy ourselves as to the identity of the person making the request. Accordingly, we require you to provide suitable proof of your identity, in the form of photographic identification (such as Passport or Driving Licence), plus an original utility bill to verify your home address.

Also, in order to assist the Multi Academy Trust in locating the information which you are seeking in a timely and efficient manner, you should provide as much information as possible as to the type of data which you are seeking, the period during which the data has been held, the persons or departments who are likely to be holding this data and the school where such persons or departments are based.

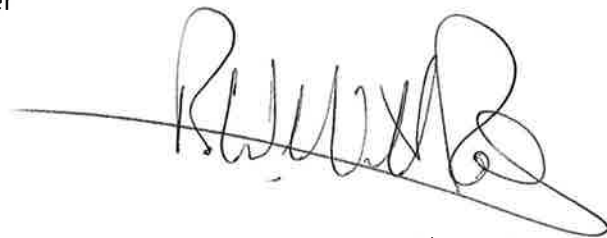
Please send the completed form and any necessary evidence (as appropriate) to The Data Protection Officer, Torquay Boys' Grammar School, Shiphay Manor Drive, Torquay, TQ2 7EL.

We will endeavour to respond to your request as soon as reasonably practicable.

Regards

Mr K Smith

Data Protection Officer



12th November 2018