The GORSE Academies Trust
c/o The Stephen Longfellow Academy
Phoenix House
Global Avenue
Leeds
LS11 8PG
0113 487 8888
info@tgat.org.uk
www.tgat.org.uk

The GORSE Academies Trust Data-Protection policy

Designated Person: Strategic Lead Officer

Reviewed by: Policy Committee

Date: 09/06/2021

Version: 1.1

DATA PROTECTION POLICY

The following amendments have been made to this (2021) version of the policy:

Introduction	Polices in conjunction updated
Section 2	Up to date address details added
Section 3	Updated TGAT structure added
Full document	Updated to reference post-EU exit wording
Full document	Updated to reference full data-protection scope (previous version was more aligned to GDPR specific wording
Full document	Updated in light of feedback from May 2021 GDPR external audit
Appendices	3 x appendices added to support section 3

This policy should be read in conjunction with the following policies:

- TGAT IT Security policy
- TGAT Data-Retention policy
- TGAT GDPR Training policy
- TGAT Subject Access Request policy
- TGAT Clear Desk/Clear Screen policy
- TGAT Data Protection Impact Assessment (DPIA) policy

1. Introduction

1.1 Background to the UK Data Protection Laws

The General Data Protection Regulation replaced the previous European data protection laws in 2018. Following the 1st of January 2021 the GDPR was adapted to the UK in a new variant called the UK GDPR, which is used, in conjunction with the Data Protection Act 2018 the Privacy & Electronic communication regulations & The Freedom of Information Act, within the United Kingdom.

1.2 Definitions used by the organisation (drawn from the UK Data Protection Laws)

1.2.1 **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.

1.2.2 **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.

1.2.3 **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 UK law, the controller or the specific criteria for its nomination may be provided for under UK law.

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

1.2.5 **Processing** – any operation or set of operations which is performed on personal data or on sets of personal data, whether 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.

1.2.6 **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 behaviour. 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.

1.2.7 **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 within a 72-hour period to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject. TGAT will also monitor and drive continual-improvement from the highlighting and management of 'near misses' related to data breaches (where a risk has been identified without a breach occurring)

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

1.2.9 **Child –** The Data Protection laws define a child as anyone under the age of 16 years old, although the age of consent for internet-based social services (ISS) data-processing in the UK is defined as 13. Consent for data-processing, aside from ISS is defined at 12 years and older within the UK. 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. Where a child is aged 12+ years in the UK the consent of the child may be required for some elements of data-processing. As an example in the event of a Subject Access Request (SAR) the consent of the child, as the data-subject, must be obtained prior to release of data.

1.2.10 **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.

1.2.11 **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. Policy statement

2.1 The Board of Directors and Senior Leaders of The GORSE Academies Trust (TGAT), located at:

The GORSE Academies Trust
C/O The Stephen Longfellow Academy
Phoenix House
Global Avenue
Leeds
LS11 8PG

are committed to compliance with all applicable UK Data-Protection laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information TGAT collects and processes.

2.2 Compliance with UK Data-Protection laws is described by this policy and other relevant policies such as the Information Security Policy, along with connected processes and procedures.

2.3 UK Data-Protection laws and this policy apply to all TGAT's personal data processing functions, including those performed on students', parents' and employee's personal data, and any other personal data the organisation processes from any source.

2.4 The Data Privacy Manager (which is a component of the role of the Strategic Lead Officer) is responsible for reviewing the Record of Processing Activities annually in the light of any changes to TGAT's activities and to any additional requirements identified by means of data protection impact assessments. This register needs to be available on the supervisory authority's request.

2.5 This policy applies to all employees/staff (permanent, temporary or casual) of TGAT (this may include outsourced suppliers). Any breach of UK Data-Protection laws will be dealt with under TGAT's 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.

2.6 Partners and any third parties working with or for TGAT, 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 TGAT without having first entered into a data confidentiality agreement, which imposes on the third-party obligations no less onerous than those to which TGAT is committed, and which gives TGAT the right to audit compliance with the agreement.

2.7 Data Protection Officer (DPO) – TGAT has appointed a DPO to oversee the data-protection strategy and performance of the Trust. The DPO is an external contractor, and legal expert in data-protection, to the organisation and works alongside the Data Privacy Manager to:

- Ensure that policy is compliant to legislation
- Ensure that operational performance is in line with best practice
- Provide specialist legal advice as necessary
- Scrutinise Data Privacy Impact Assessments

2.8 TGAT retains the services of a data-protection subject matter expert to further support the development of TGAT strategy and operational performance, including:

- Development of training material
- Audit of operational systems and performance
- Alignment with sector best-practice

3. Responsibilities and roles under the UK Data-Protection Laws

3.1 TGAT is a data controller and data processor under the UK Data-Protection Laws.

3.2 Senior Leaders and all those in managerial or supervisory roles throughout TGAT are responsible for developing and encouraging good information handling practices within TGAT.

3.3 The Data Privacy Manager is accountable to the Board of Directors of TGAT for the management of personal data within TGAT and for ensuring that compliance with

data protection legislation and good practice can be demonstrated. This role is delegated to the Strategic Lead Officer, with support from the Deputy Strategic Lead. This accountability includes:

3.3.1 development and implementation of the UK Data-Protection laws as required by this policy.

3.3.2 security and risk management in relation to compliance with the policy.

3.4 The Data Privacy Manager, who the Board of Directors considers to be suitable, has been appointed to take responsibility for TGAT's compliance with this policy on a day-today basis and, in particular, has direct responsibility for ensuring that TGAT complies with the UK Data-Protection laws, as do Senior Leaders in respect of data processing that takes place within their area of responsibility.

3.5 The Data Privacy Manager has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and are the first point of call for employees/staff seeking clarification on any aspect of data protection compliance.

3.6 TGAT has a defined data organisational structure with clear lines of accountability for strategy, operational control and scrutiny of data-protection activities, this can be viewed in appendix 1.

3.7 TGAT has a dedicated Data-Protection and Cyber-Security Steering Group (comprising of the external DPO, COO, Strategic Lead Officer, Deputy Strategic Lead & IT Operations Director & IT Networks & Security Director), who are responsible for the strategic direction of the Trust. The terms of reference for this group can be viewed in appendix 3.

3.8 Compliance with data protection legislation is the responsibility of all employees/staff of TGAT who process personal data.

3.9 TGAT's GDPR Training Policy sets out specific training and awareness requirements in relation to specific roles and employees/staff of TGAT generally.

3.10 Employees/Staff of TGAT are responsible for ensuring that any personal data about them and supplied by them to TGAT is accurate and up to date.

4. Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in the UK Data-Protection laws. TGAT's policies and procedures are designed to ensure compliance with the principles.

4.1 **Personal data must be processed lawfully, fairly and transparently**

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

Fairly – for processing to be fair, the data controller must 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.

UK Data-Protection laws have increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' requirement.

Transparently – UK Data-Protection laws include rules on giving privacy information to data subjects. 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.

TGAT's Privacy Notice is published on the TGAT's website, is linked to all Trust establishment websites, and can be found in appendix 2

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

4.1.1 the identity and the contact details of the controller and, if any, of the controller's representative.

4.1.2 the contact details of the Data Privacy Manager.

4.1.3 the purposes of the processing for which the personal data are intended as well as the legal basis for the processing.

4.1.4 the period for which the personal data will be stored.

4.1.5 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.

4.1.6 the categories of personal data concerned.

4.1.7 the recipients or categories of recipients of the personal data, where applicable.

4.1.8 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.

4.1.9 any further information necessary to guarantee fair processing.

4.2 **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 TGAT's Record of Processing Activities.

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

4.3.1 The Data Privacy Manager is responsible for ensuring that TGAT does not collect information that is not strictly necessary for the purpose for which it is obtained.

4.3.2 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 notice and approved by the Data Privacy Manager.

4.3.3 The Data Privacy Manager will ensure that, on an annual basis all data collection methods are reviewed by internal audit to ensure that collected data continues to be adequate, relevant and not excessive.

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

4.4.1 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.

4.4.2 The Data Privacy Manager is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

4.4.3 It is also the responsibility of the data subject to ensure that data held by TGAT 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.

4.4.4 Employees/staff are required to notify TGAT of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of TGAT to ensure that any notification regarding change of circumstances is recorded and acted upon.

4.4.5 The Data Privacy Manager 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.

4.4.6 On at least an annual basis, the Data Privacy Manager will review the retention dates of all the personal data processed by TGAT, 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 in line with the UK Data-Protection laws.

4.4.7 The Data Privacy Manager is responsible for responding to requests for rectification from data subjects within one month. This can be extended to a further two months for complex requests. If TGAT decides not to comply with the request, the Data Privacy Manager 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.

4.4.8 The Data Privacy Manager 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.

4.5 **Personal data must be kept in a form such that the data subject can be identified only if is necessary for processing.**

4.5.1 Personal data will be retained in line with the Retention of Records policy and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

4.5.2 The Data Privacy Manager must specifically approve any data retention that exceeds the retention periods defined in Retention of Records Procedure and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

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

The Data Privacy Manager will carry out a risk assessment taking into account all the circumstances of TGAT's controlling or processing operations.

In determining appropriateness, the Data Privacy Manager should also consider the extent of possible damage or loss that might be caused to individuals if a security

breach occurs, the effect of any security breach on TGAT itself, and any likely reputational damage.

When assessing appropriate technical measures, the Data Privacy Manager will 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
- Identifying appropriate international security standards relevant to TGAT

When assessing appropriate organisational measures the Data Privacy Manager will consider the following:

- The appropriate training levels throughout TGAT
- 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
- Restricting the use of employee's own personal devices being used in the workplace
- 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 UK

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.

4.7 **The controller must be able to demonstrate compliance with other data-processing principles (accountability)**

UK Data-Protection laws include provisions that promote accountability and governance. These complement the transparency requirements. The accountability principle requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

TGAT 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, Data Protection Impact Assessments (DPIAs), breach notification procedures and incident response plans.

4.8 **Biometric Data**

The GORSE Academies Trust collect biometric fingerprints from staff and students to support the use of Cashless Catering and Printing in our academies. The solution used by the Trust creates a random string using an algorithm and does not store an image of the fingerprint at any point. Biometric data is only collected once written permission has been given by the individual (if they are over 18 years old) or a legal guardian (if they are under 18 years old) and the individual consents to the taking of their fingerprint (verbal or written). All legal guardians are notified of the Trusts intention to use biometrics and have the opportunity to decline its use (this over rules any consent received). Biometric data is destroyed upon the request of a legal guardian or in the event of the individual requesting us to do so (written or verbal). All biometric data is destroyed when an individual leaves employment/education with the Trust.

5. Data subjects' rights

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

5.1.1 To make subject access requests regarding the nature of information held and to whom it has been disclosed.

5.1.2 To prevent processing likely to cause damage or distress.

5.1.3 To prevent processing for purposes of direct marketing.

5.1.4 To be informed about the mechanics of automated decision-taking process that will significantly affect them.

5.1.5 To not have significant decisions that will affect them taken solely by automated process.

5.1.7 To take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data.

5.1.8 To request the supervisory authority to assess whether any provision of the GDPR has been contravened.

5.1.9 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.

5.1.10 To object to any automated profiling that is occurring without consent.

5.2 TGAT ensures that data subjects may exercise these rights:

5.2.1 Data subjects may make data access requests via a Subject Access Request Procedure.

5.2.2 Data subjects have the right to complain to TGAT 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.

6. Consent

6.1 TGAT 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.

6.2 TGAT 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.

6.3 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.

6.4 For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

7. Security of data

7.1 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, in line with the TGAT clear desk/screen policy, 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 corporate requirements in the Access Control Policy; and/or
- stored on (removable) computer media which are encrypted

7.2 Care must be taken to ensure that sensitive information displayed on PC screens and terminals is not visible except to authorised employees/staff of TGAT. 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.

7.3 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation.

7.4 Personal data may only be deleted or disposed of in line with the Retention of Records Procedure. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as per UK Data-Protection laws before disposal.

7.5 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, unless using TGAT secure remote systems covered under the Acceptable User Agreement.

8. Disclosure of data

8.1 TGAT must ensure that personal data is only disclosed to third parties when there is a lawful basis for doing so. For example where there is a lawful basis to disclose including as part of a prevention or investigation of a crime, part of an assessment or collection of taxes or in the vital interests of the data subject. All employees/staff should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether disclosure of the information is relevant to, and necessary for, the conduct of TGAT's business.

8.2 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 Privacy Manager.

9. Retention and disposal of data

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

9.2 TGAT 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.

9.3 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 TGAT has to retain the data.

9.4 TGAT's data retention and data disposal policy (Storage Removal Procedure) will apply in all cases.

9.5 Personal data must be disposed of securely in accordance with UK Data-Protection laws and '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.

10. Data transfers

10.1 All exports of data from within the UK to non-UK countries (referred to in UK Data-Protection law 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 UK is prohibited unless one or more of the specified safeguards, or exceptions, apply:

10.1.1 Adequacy regulations

The UK can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances no authorisation is required. Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as having met the conditions of the adequacy regulations. A list of countries that currently satisfy the adequacy regulations under the UK GDPR can be seen at:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/#adequacy

10.1.2 UK Binding corporate rules (UKBCR)

TGAT may adopt approved binding corporate rules for the transfer of data outside the EU. This requires submission to the relevant supervisory authority for approval of the rules that TGAT is seeking to rely upon.

10.1.3 **Standard Contractual Clauses**

TGAT may adopt approved model contract clauses for the transfer of data outside of the UK. If TGAT adopts the model contract clauses approved by the Information Commissioner's Office, there is an automatic recognition of adequacy.

10.1.4 **Exceptions**

In the absence of an adequacy decision, binding corporate rules and/or standard contractual clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards
- the transfer is necessary for the performance of a contract between the data subject and the controller, or the implementation of pre-contractual measures taken at the data subject's request
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person
- the transfer is necessary for important reasons of public interest
- the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent

11. Information asset register/data inventory

11.1 TGAT has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its UK Data-Protection compliance activities. TGAT's 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 TGAT throughout the data flow
- key systems and repositories
- any data transfers; and
- all retention and disposal requirements

11.2 TGAT is aware of any risks associated with the processing of particular types of personal data.

11.2.1 TGAT assesses the level of risk to individuals associated with the processing of their personal data. Data Privacy Impact Assessments (DPIA's) are carried out in relation to the processing of personal data by TGAT, and in relation to processing undertaken by other organisations on behalf of TGAT. These DPIA's are completed in line with the TGAT Data-Privacy Impact Assessment policy and are reviewed and signed-off by the DPO.

11.2.2 TGAT shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

11.2.3 Where a type of processing, in particular using new technologies and considering the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, TGAT shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.

11.2.4 Where, because of a DPIA it is clear that TGAT is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether TGAT may proceed must be escalated for review to the Data Privacy Manager.

11.2.5 The Data Privacy Manager shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority.

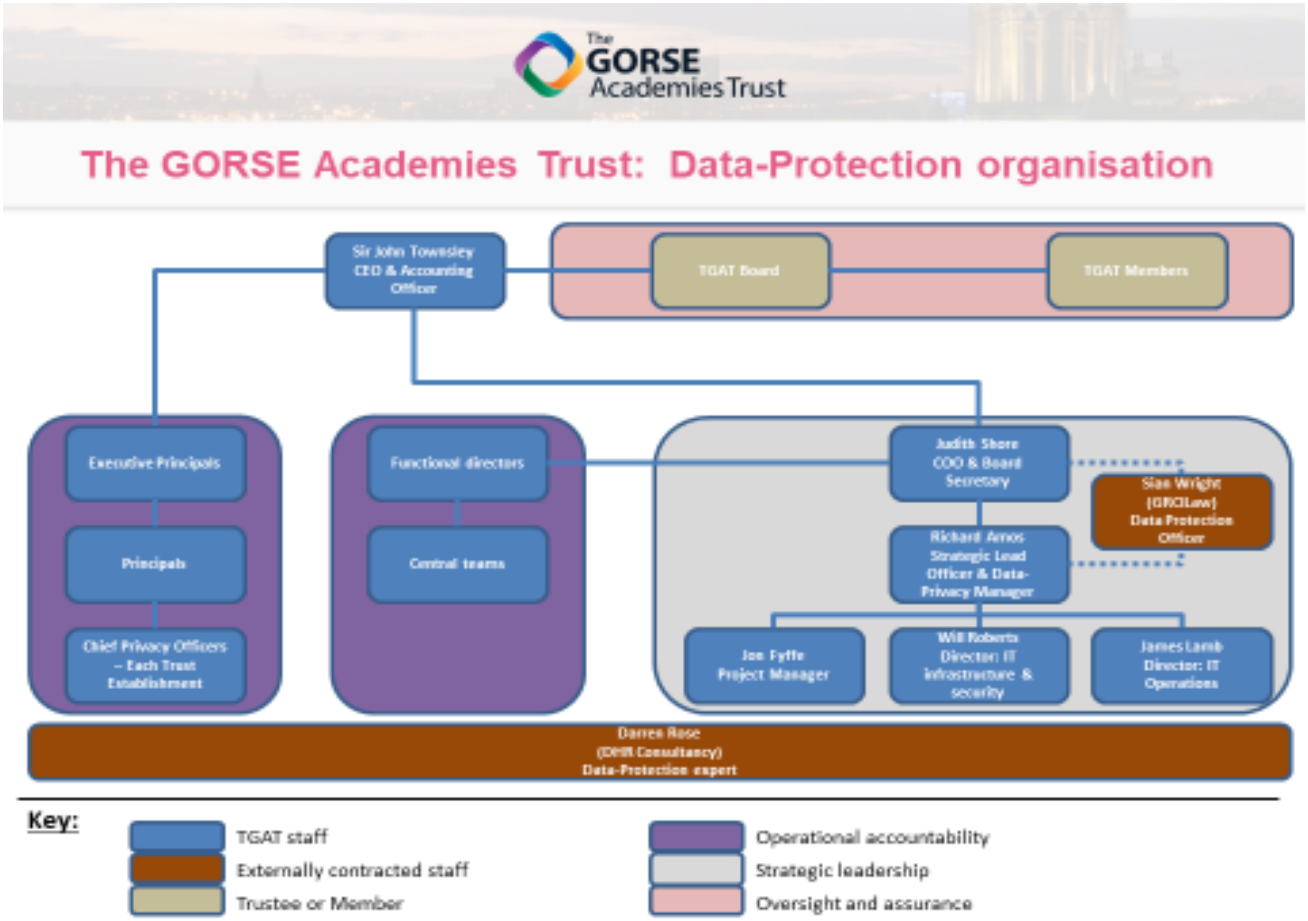
11.2.6 Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to the requirements of UK Data-Protection Laws.

Document control:

Reason for version change:	Planned cycle review	Version number:	1.1
Date of Approval:	09/06/21	Approved by:	Policy Committee
Target Audience:	All staff	Date issued:	09/06/21

APPENDIX 1

TGAT Data-Protection organisational structure



The GORSE Academies Trust
c/o The Stephen Longfellow Academy
Phoenix House, Global Avenue, Leeds, LS11 8PG

Data-protection activity within The GORSE Academies Trust (TGAT) is managed at three distinct levels:

Strategic oversight

- Aligning data-protection activity to relevant legislation and specific educational policy
- Utilising external expertise on the form of the TGAT Data Protection Officer, who is an external legal expert
- Utilising external expertise through the use of a retained data-protection consultant, a certified member of IAPP
- Leading on data-protection policy development, training development and communication
- Tracking compliance on regulated activity (for example Subject access requests) & training delivery (including new starte r induction)
- Overseeing impact assessment one new or amended use of personal data
- Assuring IT system compliance and cyber-security controls
- Analysing trends to ensure continual improvement of process, policy, training & communication
- Presenting performance and trends to the executive team and board, through a termly dashboard
- Leadership of CPO group on a half-termly basis – ensuring timely and appropriate communication of policy and cascading best-practice
- Engagement with the Information Commissioners office as appropriate

Operational accountability:

- Principals/equivalents have establishment level accountability for data-protection, with Executive Principal accountability at 'phase-level'
- A dedicated Chief Privacy Officer (CPO) exists for all Trust establishments – where necessary, due to size/scope, there are multiple CPO's
- CPO's report directly to the principal/equivalent for data-protection activity and are usually a member of the senior leadership team
- CPO's are responsible for:
    - Compliance to relevant legislation & TGAT policy by their staff
    - Training and communication for their site/staff
    - Management of data requests (eg SAR's or FOI requests) at their establishment
    - Implementation of any new or amended policies

Oversight & Assurance:

- TGAT Board: assuring the robustness of the strategic direction and the operational performance of the Trust
- Local Governing Body (LGB): assuring the operational performance of the individual establishment

Appendix 2

Link to Current TGAT Privacy notice is below:

https://www.tgat.org.uk/privacy-notice/

Appendix 3

The GORSE Academies Trust

Terms of Reference – Data-Protection & Cyber Security Steering Group

		Members:
Meeting Frequency:	**Termly**	**Judith Shore: COO** **Richard Amos: Strategic Lead Officer** **Sian Wright: Data-Protection officer** **Will Roberts: Director of IT infrastructure & security** **James Lamb: Director of IT Operations** **Jon Fyffe: Project Manager**
Key Inputs	• **Termly Data-Protection summary report (provided by Project Manager)** • **Termly Cyber-security summary report (provided by Director of IT infrastructure & Security)** • **Specific reports on any data-protection or cyber-security incidents in the last period** • **Cyber-security audit report (as appropriate in the audit cycle)** • **Sector best practice guidance and legal perspective (provided by DPO)**	
Key Outputs:	• **Agreed actions to take forward into the Data-Protection/GDPR CPO group for the following term** • **Agreed actions to take forward into the policy review cycle for the following term** • **Agreed actions to take forward into the IT infrastructure & security plan** • **Agreed actions to take forward into the IT operations plan** • **Updates to TGAT Executive team & TGAT Board as appropriate – including annual report to Finance, Audit & Risk committee**	

	Key principles/accountabilities:
1	**TGAT remains adequately protected from threats to IT infrastructure & personal data, mitigating commercial, reputational & operational risk**
2	**TGAT organisational, staff, pupil/student and parent/carer data is secure and managed within relevant legislation and policy**
3	**TGAT Data-Protection and cyber-security activity is integrated and aligned in terms of policy, process & operations**
4	**TGAT Data-Protection policy is aligned to current legislation and practice and that this meeting effectively drives operational planning**
5	**TGAT cyber-security policy is aligned to best practice, meets audit requirement and effectively drives IT Operational planning**
6	**TGAT remains abreast of sector wide developments and best practice, aligning TGAT policy and planning to this where necessary**
7	**TGAT staff are correctly trained and aware of responsibilities/accountabilities based on their job role**
8	**TGAT ensures that all data-subjects rights are upheld in one with current legislation**