The GORSE Academies Trust Access Control Policy

Designated Person: Strategic Lead Officer

Reviewed by: Policy Committee

Date: 28/04/2021

ACCESS CONTROL POLICY

1 The GORSE Academies Trust (TGAT) controls access to information on the basis of business and security requirements.

2 Access control rules and rights to applications, expressed in standard user profiles, for each user/group of users are clearly stated, together with the business requirements met by the controls.

3 The security requirements of each business application are determined by a risk assessment that identifies all information related to the application and the risks to that information.

4 The access rights to each application take into account:

a. Premises access control – unauthorised persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems are located.

b. System access control – access to data processing systems is prevented from being used without authorisation.

c. Data access control – persons entitled to use a data processing system gain access only to the data to which they have a right of access.

d. Personal data cannot be read, copied, modified or removed without authorisation.

e. The classification levels of information processed within that application and ensure that there is consistency between the classification levels and access control requirements across the systems and network(s).

f. Data protection (General Data Protection Regulations (GDPR)) and privacy, legislation and any contractual commitments regarding access to data or services.

g. The need to know principle (i.e. access is granted at the minimum level necessary for the role).

h. Everything is generally forbidden unless expressly permitted.

i. Rules that must always be enforced and those that are only guidelines.

j. Prohibition of user-initiated changes to user permissions.

k. Enforcing rules that require specific permission before enactment.

l. Any privileges that users actually need to perform their roles, subject to it being on a need-to-use and event-by-event basis.

5 TGAT has standard user access profiles for common roles.

6 The management of access rights across the network(s) is managed via the access control policy and processes.

7 User access requests are subject to formal authorisation, to periodic review and to removal.

8 Processes exist for the completion of mandatory recruitment processes prior to a member of staff being granted access to systems and networks (for example DBS checks completed).

9 Processes are in place to remove access for a member of staff when they are no longer employed by TGAT.

10 Student account creation and deletion is managed by the admissions and leaving policies – when a student no longer requires a systems/network access it will be removed.

The following policies are linked to this policy:

- TGAT Information Security policy
- TGAT Acceptable Use policy
- TGAT Data-Protection policy
- TGAT Personal Data-Retention policy
- TGAT Safer Recruitment policy

Document control:

Reason for version change:	Review Cycle	Version number:	1.0
Date of Approval:	28/04/2021	Approved by:	Policy Committee
Target Audience:	All Staff/Students/Parents/carers – via Academy websites	Date issued:	28/04/21

APPENDIX

Insert any appendices from this point