



GESHER SCHOOL
ENGAGE EMPOWER EDUCATE

Access Control Policy

2020-2021

Date	Review Date	Data Protection Officer	Data Privacy Officer
October 2020	October 2021	Judicium Consulting Limited	Dafna Hyman

1. Introduction

Gesher understands its obligations under the General Data Protection Regulation ('GDPR') and is committed to ensuring its staff, governors and trustees are fully trained in compliance with these regulations.

- 1 Gesher controls access to information on the basis of education 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 requirements met by the controls.
- 3 The security requirements of each 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.
 - f. Data protection (EU GDPR) and privacy legislation and 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. We prohibit user-initiated changes to information classification labels.
 - j. We prohibit user-initiated changes to user permissions.
 - k. We enforce rules that require specific permission before enactment.

- I. Any privileges that users actually need to perform their roles are subject to it being on a need-to-use and event-by-event basis.
- 5 Gesher has standard user access profiles for common roles in Gesher School and the Gesher Trust.
- 6 Management of access rights across the network is strictly limited.
- 7 User access requests, authorisation and administration are segregated.
- 8 User access requests are subject to formal authorisation, to periodic review and to removal.

2. Review of Policy

As part of our wider Data Protection Procedures, this Policy will be reviewed on an ongoing basis by the Gesher School senior management team and Gesher Governors.