The GORSE Academies Trust
c/o John Smeaton Academy
Smeaton Approach
Barwick Road
Leeds
LS15 8TA
0113 487 8888
info@tgat.org.uk
www.tgat.org.uk

The GORSE Academies Trust: Information Security Policy

Designated Person:	Strategic Lead Officer
Reviewed by:	Policy Committee
Date:	20/10/2021
Version:	1.0

INFORMATION SECURITY POLICY

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

c/o John Smeaton Academy
Smeaton Approach
Barwick Road
Leeds
LS15 8TA

are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout their organisation. In particular, business continuity and contingency plans, data back-up procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental.

TGAT aims to achieve specific, defined information security objectives, which are developed in accordance with the business objectives, the context of the organisation and the results of risk assessments.

This policy will be regularly reviewed to respond to any changes in the risk assessment.

This policy is supported by the following policies:

- TGAT IT Security Policy (and associated technical policies)
- TGAT Data-Protection Policy
- TGAT Business Continuity Policy

In this policy, 'information security' is defined as:

Preserving:
This means that Senior Leaders, all full time or part time employees/staff, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities to preserve information security and to report security breaches.

The availability:
This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The computer network must be resilient and the Trust must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. There must be appropriate business continuity plans.

Confidentiality:
This involves ensuring that information is only accessible to those authorised to access it and therefore to preventing both deliberate and accidental unauthorised access to TGAT's information and its systems.

And Integrity:
This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial or complete destruction or unauthorised modification, of either physical assets or electronic data. There must be appropriate contingency and data back-up plans and security incident reporting. TGAT must comply with all relevant data-related legislation in those jurisdictions within which it operates.

of the Physical Assets:
The physical assets of TGAT including, but not limited to, computer hardware, data cabling, telephone systems, filing systems and physical data files.

and Information Assets:
The information assets include information printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, website(s), extranet(s), intranet(s), PCs, laptops, mobile phones and PDAs, as well as on CD ROMs, floppy disks, USB sticks, backup tapes and any other digital or magnetic media, and information transmitted electronically by any means. In this context, data also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc).

A **security breach** is any incident or activity that causes, or may cause, a break down in the availability, confidentiality or integrity of the physical or electronic information assets of TGAT.

Document control:

Reason for version change:	Update Due	Version number:	1.0
Date of Approval:	20/10/21	Approved by:	Policy Committee
Target Audience:	External – All websites	Date issued:	20/10/21