Information Security Policy
GDPR_REC_5.2

Policy Version Control	
Policy type	Academy Trust
Policy prepared by (name and designation)	Tristen Coad DPO
Last review date	1st July 2021
Description of changes	New
Date of Board of Trustees approval	8th July 2021
Date released	13th September 2021
Next review date	Summer 2022

Document Owner & Approval

The Director of Operations is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

A current version of this document is available to all members of staff on the school's Shared Area.

This manual was approved by the Board of Trustees on 8th July 2021 and is issued on a version controlled basis under the signature of the Trustee with responsibility for GDPR.

Signature: Date:

The Board of Trustees and management of Lingfield Education Trust, located at Corporation Road Primary School Darlington, which operates in the education sector, are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout their organisation in order to preserve its competitive edge, cash-flow, profitability, legal, regulatory and contractual compliance and commercial image. Information and information security requirements will continue to be aligned with Lingfield Education Trusts goals and the ISMS is intended to be an enabling mechanism for information sharing, for electronic operations and for reducing information-related risks to acceptable levels.
In particular, business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy. Control objectives for each of these areas are contained in Lingfield Education Trust's central document repository.

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

All Employees of Lingfield Education Trust and certain external parties identified are expected to comply with this policy and with the ISMS that implements this policy. All Staff, and certain external parties, will receive appropriate training. The consequences of breaching the information security policy are set out in the disciplinary policy and in contracts and agreements with third parties.

This policy will be reviewed to respond to any changes in the risk assessment plan at least annually.

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

Preserving

This means that management, all full time or part time Staff, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches and to act in accordance with the requirements of the PIMS. All Staff will receive awareness training and more specialised Staff will receive appropriately specialised information security training.

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 Lingfield Education 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 Lingfield

Education Trust information and proprietary knowledge and its systems including its network(s), website(s), extranet(s), and e-commerce 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 including for network(s), website(s) and data backup plans and security incident reporting. Lingfield Education Trust must comply with all relevant data-related legislation in those jurisdictions within which it operates.

of the physical (assets)

The physical assets of Lingfield Education Trust 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 Lingfield Education Trust.

POLICY REVIEW DATE: Summer 2022