Preface and document control

This document is intended to provide information security policy, procedure, standards or guidance in respect of **St Anne's College** and shall be reviewed at least annually to ensure validity.

Neither all nor part of this document shall be reproduced or released by a recipient without the explicit authorisation of the stated document owner.

1 Purpose....4
2 Scope....4
3 Objectives....4
4 Information Security Policy Framework (ISPF)....4
5 Responsibilities....5
6 Compliance....5
7 Review and Development....5

1 Purpose

This policy outlines **St Anne's College's** approach to information security management and provides the guiding principles and responsibilities to ensure **St Anne's College's** security objectives are met.

2 Scope

This policy is applicable across **St Anne's College** and individually applies to:

- all individuals who have access to **St Anne's College** information and technologies;
- all facilities, technologies and services that are used to process **St Anne's College** information;
- information processed, in any format, by **St Anne's College** pursuant to its operational activities;
- internal and external processes used to process **St Anne's College** information; and
- external parties that provide information processing services to **St Anne's College**.

3 Objectives

St Anne's College's objectives for information security are that:

- a culture is embedded to ensure all teaching, research and administration activities consider information security;
- individuals are aware and kept informed of their information security responsibilities;
- information risks are identified, managed and mitigated to an acceptable level;
- authorised users can access information securely to perform their roles;
- facilities, technologies and services adequately balance usability and security;
- implemented security controls are pragmatic, effective and measurable;
- contractual, regulatory and legal obligations relating to information security are met; and
- incidents are effectively managed and resolved, and learnt from to improve information security.

4 Information Security Policy Framework (ISPF)

Information is critical to **St Anne's College** operations and failure to protect information increases the risk of financial and reputational losses. **St Anne's College** is committed to protecting information, in all its forms, from loss of **confidentiality**, **integrity** and **availability** ensuring that:

- all staff complete information security awareness training;
- information security risk is adequately managed and risk assessments on IT systems and business processes are performed where appropriate;
- all relevant information security requirements of **St Anne's College** are covered in agreements with any third-party partners or suppliers, and compliance against these is monitored;
- appropriate information security controls are implemented to protect all IT facilities, technologies and services used to access, process and store **St Anne's College** information;
- all information security incidents are reported in a timely manner via appropriate management channels, information systems are isolated, and incidents properly investigated and managed;
- Information Asset Owners are identified for all **St Anne's College** information assets, assets are classified according to how critical and sensitive they are, and rules for their use are in place; and

- Information security controls are monitored to ensure they are adequate and effective.

To provide the foundation of a pragmatic information security framework, **St Anne's College** will implement a set of minimum information security controls, known as the baseline, either as published by the University's Information Security team or of equivalent strength. Where research, regulatory or national requirements exceed this baseline, controls will be increased at necessary service or project level. Where it is not possible or practicable to meet the baseline, exceptions will be documented to justify the deviation and appropriate compensating controls will be put in place. The baseline will support **St Anne's College** in achieving its information security objectives.

The policy and the baseline shall be communicated to users and relevant external parties, and linked to from the website.

5 Responsibilities

The following bodies and individuals have specific information security responsibilities:

- **The Principal** is accountable for the effective implementation of this information security policy, and supporting information security rules and standards, within **St Anne's College**.
- **Governing Body** has executive responsibility for information security **St Anne's College**. Specifically, **Governing Body** has responsibility for overseeing the management of the security risks to **St Anne's College's** staff and students, its infrastructure and its information.
- **The Treasurer and Finance Director,** working with the IT & Data Security Committee, is responsible for establishing and maintaining **St Anne's College's** information security management framework to ensure the availability, integrity and confidentiality of **St Anne's College's** information. **The Treasurer and Finance Director** will lead on the definition and implementation of **St Anne's College's** information security arrangements.
- **The IT & Data Security Committee** was established by the College to support preparation for GDPR and to ensure compliance with regulation and good practice in relation to data protection.
- **The Data Protection Officer (DPO)** will inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws. She / he will monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits. She / he is the first point of contact for supervisory authorities and for individuals whose data is processed.
- **Users** are responsible for making informed decisions to protect the information that they process.

6 Compliance

St Anne's College shall conduct information security compliance and assurance activities, facilitated by the Conference of Colleges Information Security Working Group, to ensure information security objectives and the requirements of the ISPF are met. Wilful failure to comply with the policy and baseline will be treated extremely seriously by **St Anne's College** and may result in enforcement action on a group and/or an individual.

7 Review and Development

This policy, and supporting ISPF documentation, shall be reviewed and updated by **The Treasurer and Finance Director,** working with the IT & Data Security Committee and the **DPO**, and approved by **Governing Body** on an annual basis to ensure that they:

- remain operationally fit for purpose;
- reflect changes in technologies;

- are aligned to industry best practice; and
- support continued regulatory, contractual and legal compliance.

NOTE: This Information Security Policy should be read alongside the College's Acceptable Use Policy, the Mobile Device Policy and other policy documents and advice.