Information Security Policy

1 Purpose

This policy outlines the approach of Lincoln College (the "College") to information security management and provides the guiding principles and responsibilities to ensure the College's security objectives are met.

2 Scope

This policy is applicable across the College and individually applies to:

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

3 Objectives

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

- 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;
- College, University and other sensitive information will be stored on College or University systems unless specific third-party agreements are in place;
- all relevant information security requirements of the 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 the 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 the 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, the 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 the 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 Governing Body** is accountable for the effective implementation of this information security policy, and supporting information security rules and standards, within the College. Specifically, Governing Body has responsibility for overseeing the management of the security risks to the College's staff and students, its infrastructure and its information.

- **The IT Manager** is responsible for establishing and maintaining the College's information security management framework to ensure the availability, integrity and confidentiality of the College's information.
- **Users** are responsible for their implementation of information security requirements and for making informed decisions to protect the information that they process.

6 Compliance

In addition to this Information Security Policy users are required to comply with the College's mobile devices policy below and the College's Acceptable Use policy below. The 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 these policies will be treated seriously by the 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 Bursar 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.

Mobile Device Security Policy

8 Purpose

This policy outlines the approach of Lincoln College (the "College") to securing mobile devices such as smartphones, tablets and computer laptops, and provides guiding principles and responsibilities to ensure College's security objectives are met.

9 Scope

This policy is applicable across the College and individually applies to:

- all individuals who have access to the College's information and technologies;
- "mobile device" applies to any mobile hardware that is used to access or store College resources, whether the device is owned by the user or by the College.

10 Mobile Device Security

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

- It must be protected from unauthorised access by at least a 4-digit PIN or a passphrase and be configured to ensure an automatic lock after a period of inactivity.
- All devices are encrypted using appropriate and approved methods such as Bitlocker or Filevault.
- Only trustworthy applications from reputable sources are installed.
- It is configured to receive software updates from the manufacturer and other 3rd parties and updates are installed within one week of being released.
- It is prohibited to connect to the College network any mobile device that has undergone a 'jailbreak' procedure.
- Mobile devices should not be used to carry sensitive data for any longer then absolutely necessary and must be encrypted to protect any data that is on the device.
- Any mobile device that is stolen or lost must be reported to the IT team immediately if it has access to College data. Reporting loss or theft to the College Lodge out of normal working hours is acceptable, but effort must be made to contact the IT Staff so that the risk of a data breach can be mitigated.
- Connection to College networks from mobile devices must be via an encrypted link using the University VPN service.

Where research, regulatory or national requirements exceed these baseline criteria, controls must be increased as necessary. Where it is not practicable to meet the baseline, exceptions will be documented to justify the deviation and appropriate compensating controls will be put in place.

11 Responsibilities

The following bodies and individuals have specific information security responsibilities:

- **Governing Body** has responsibility for information security within the College. Specifically, Governing Body has responsibility for overseeing the management of the security risks to the College's staff and students, its infrastructure and its information.
- **The IT Manager** is responsible for establishing and maintaining the College's information security management framework and for ensuring that security guidance is available for mobile device users.
- **Users** are responsible for making informed decisions to protect the information that they process.

12 Compliance

Wilful failure to comply with the policy will be treated extremely seriously by the College and may result in enforcement action on a group and/or an individual.

13 Review and Development

This policy, and supporting documentation, shall be reviewed and updated by The Bursar 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.

23 May 2018