IT Security and Data Storage

Introduction

LIS will take all reasonable measures to ensure that their systems are secure and that data is collected, processed and stored securely.

LIS are in the process of securing a premises and selecting certain software solutions. As such, the items listed below will remain subject to updates.

IT Security

IT security will be provided at both hardware and software levels and will include the following measures, outlined below.

Local Area Network and Internet

LIS will operate a distributed network services Local Area Network (LAN) at its premises, served by an Internet Service Provider (ISP) with a business grade, secure internet connection (e.g., JANET). Under a Service Level Agreement, the ISP will monitor the connection to prevent Distributed Denial of Service incidents and other suspicious/debilitating activity.

Hardware Security

The ISP will provide a physical hardware router/firewall with associated Access Control Lists (ACLs) for restricting areas of the network from unauthorized users, as well as guarding against network attacks

LIS will also configure a demilitarized zone (DMZ), to segment and secure its LAN from internet traffic. A fibre 'backbone' will serve the LAN with secure network switching incorporating the following features:

- Embedded security for encrypting network communications and protecting data that travels to and from the switch
- Access control lists (ACLs) for restricting areas of the network from unauthorized users as well as guarding against network attacks
- Virtual LANS (vLANs) for segmenting the network into separate work groups or creating a guest work group for giving visitors limited access to the network and to the Internet

LIS will configure a Wireless Network comprising of access points using wireless traffic encryption (WEP/WPA/WPA2). There will be a secure network for student and staff access, as well as a segregated unsecure network for guests.

Software security

LIS will configure secure Domain Name Services (DNS) routing and will consider the use of DNS security services (example OpenDNS) to provide the following security features

- Built-in protection for malicious phishing & malware domains
- Customizable content filtering

- Retention of up to 12 months of internet statistics from the LAN

LIS' corporate email provider (Example Google Business Email) will provide anti-spam and anti-virus e-mail filtering to protect against phishing, malware and ransomware incidents. Scanning will include malicious URLs hidden within emails and their attachments.

SaaS solution security

LIS will deploy a number of cloud-based software solutions (example Ellucian Quercus student management system, Aula Learning Management System) and will ensure that all such systems are correctly secured via 'SSL' certificates. The associated SSL certificates will ensure that internet traffic is authenticated and verified. This will also provide data encryption so that sensitive information exchanged via websites cannot be intercepted and read by anyone other than the intended recipient.

Mobile device policy

LIS will implement a mobile device policy for all corporate devices and will configure dual factor authentication, to ensure that access to LIS data and services from mobile devices is secure.

SaaS security

When selecting SaaS solutions/vendors LIS will, where appropriate, pay close attention to the standards outlined in the National Cyber Security Centre SaaS security principles.

Data storage

LIS will utilise a cloud file storage solution. The LAN will include a local file server for storage of data. LIS will ensure that local data is secured by:

- Ensuring that the file server is physically secure
- Server hard drives are encrypted
- File servers are fully patched and up to date
- Security protocols (example NTFS) are used to restrict file and folder access to specific groups or individual users
- An auditing function is configured to see who is attempting to read, write, or delete confidential files and folders

The LAN fileserver will be configured to synchronise local files to a secure cloud storage location (e.g., Amazon Web Services).

Data Backup

All LIS data is stored within SaaS solutions with their own backup policies and strategies. The Head of Digital will maintain a list of these policies and ensure that backups are appropriately taken through each. Every new process must be assessed for backup capabilities before a decision to use them is taken.

Version control

Name of policy/procedure:	**IT Security and Data Storage**
Document owner:	**Kestral Gaian, Head of Digital**
Date Originally Created:	**07/2019**
Related documents: (e.g. associated forms, underpinning processes, related policies or overarching policies)	**IT Disaster Recovery Plan**

Version Control			
Version	**Author**	**Date**	**Brief summary of changes**
1	Jasper Joyce (Director of Finance and Operations)	15/07/2019	Original draft
2	Chris Colnaghi (External IT consultant)	02/08/2019	Updated technical details of IT security principles
3	Hannah Kohler (Director of Admissions and Student Support)	02/08/2019	Minor wording changes
4	Jasper Joyce (Director of Finance and Operations)	08/08/2019	Minor wording changes
5	Kestral Gaian (Chair of the Data & IT Working Group)	20/10/2021	Updating policy and positioning to match current status.
6	Kestral Gaian (Head of Digital)	23/11/2022	Updating wording around working groups after merge into Learning Resources, property, Data & IT Committee.