Electronic Information Security Document

1. Introduction

1.1. Definitions

You	A third party who has engaged Us to provide services.
Us, we, our	Hubken Group Ltd registered in England and Wales with company registration number 05029965 and whose registered office address is at E-Innovation Centre, Priorslee, Telford, Shropshire, TF2 9FT.
Client Data	Data collected by the software products supported by Us (such as Totara and Moodle and as otherwise set out in our Terms of Business) and operated by you.
Data Protection Legislation	(i) unless and until the General Data Protection Regulation (EU 2016/679) (**GDPR**) is no longer directly applicable in the UK, the GDPR and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK and then (ii) any successor legislation to the GDPR or the Data Protection Act 2018.
IT	Information Technology.
Terms of Business	The terms upon which we will provide our services to you, as amended from time to time. The most recent version of which is available at http://tob.hubkengroup.com
Sensitive Data	Information that is identified as such by Data Protection Legislation and all information which is described under the “Confidential data” and “Your data” sections in our Terms of Business.
Services	The services offered by Us to assist You in the operation of the products supported by Us, as set out in our Terms of Business.
User	An authorised person connected to our IT system (include staff members and sub-contractors).

1.2. Staff Roles

This policy identifies staff with key roles. There will be occasions when the primary contact is not available and you should consult with the alternate contact, as applicable:

Role	Primary	Alternate
Infrastructure Manager	Ray Lawrence	Vicky Harper
Responsible Director	Vicky Harper	Ray Lawrence

1.3. Policy objectives

To clearly define requirements for the use of our IT facilities and data that our IT systems hold.

To ensure that Users do not unintentionally place themselves, or us, at risk of prosecution or disciplinary action, by carrying out activities which contravene current policy or legislative restrictions.

To ensure information security controls are designed to protect Users and You by maintaining:

- Confidentiality - data and information can be accessed only by those suitably authorised
- Integrity - data and information is accurate and up-to-date, and has not been deliberately or inadvertently modified from a previously approved version; and
- Availability - data and information can always be accessed.

To protect Sensitive Data and Client Data, as well as the underlying IT systems and to ensure that controls are deployed that mitigate the risk of vulnerabilities being exploited.

1.4. Policy Structure

This document is an overarching framework and evidences our commitment to apply information security controls.

Supporting policies and guidance may be developed by us to supplement this document and where we do this, we shall notify each User (where applicable). Depending upon the subject matter, supporting policies and guidance may apply across our entire business or to specific business areas, .g. Implementation, Client Relations, Infrastructure Team.

1.5. Applicability

This policy applies to all Users and includes:

- all staff employed by, or working for, or on behalf of us;
- third party contractors and consultants working for, or on behalf of us; and
- all other individuals and groups who we have granted access to our internal network or hosting platform.

The Infrastructure Manager is responsible for compliance with the policies and procedures in support of the Electronic Information Security Policy and will report non-conformance to the Responsible Director. The manager of each team is responsible for ensuring that adherence to this policy is observed within their respective department and for overseeing compliance by Users under their direction, control or supervision.

Each User is responsible for their own actions and must ensure all actions relating to the use of the IT network and the data held therein adheres to the principles and requirements of this policy.

2. Network configuration

We maintain clear separation of our internal and client facing IT systems.

- All client hosting activities are separate from the internal IT systems utilised by us for our own business purposes.
- Access to the client hosting platform is granted only to Users that require access to fulfil their staff role and is revoked when no longer needed.
- For permitted Users, specific access credentials are made available. The access credentials are held in an encrypted vault and are only valid when used in conjunction

with VPN access. VPN access is dependent upon the necessary Active Directory permissions.

- The principal areas of business and the IT systems utilised are as follows:
    - Administration and management of our business – Internal systems
    - Learning management systems – Client hosting platform
    - Work in development – Internal systems

3. Legislation and policy

3.1. Legislation

All processing of data will be processed in accordance with the Data Protection Legislation. Further information regarding our processing obligations can be found in our Terms of Business.

3.2. Data Processor or Data Controller

Both of these terms are as defined in the Data Protection Legislation.

We are both the Data Controller and Data Processor for data that we hold for the purpose of managing our business.

We are the Data Controller for data that we hold for the purpose of managing our business, but not the data processor where we have engaged a third-party processor e.g. pension administration.

When we perform actions on your behalf e.g. hosting of a site, administrative support or tasks you are the Data Controller and we act as the Data Processor. When acting as Data Processor we do not take on any of your responsibilities as Data Controller.

3.3. Confidentiality

We will keep all data (including Client Data) within IT networks that are designed to be secure and only accessible to our authorised Users.

Where appropriate, we will apply additional authorisation criteria to limit access to data.

3.4. Marketing information

We will not supply or exchange information about staff, Users or Clients to third parties for marketing purposes.

4. Risk Management

The Infrastructure Manager is responsible for the adoption of an effective and efficient environment within our business that supports the use of authorisation and authentication to obtain access to data.

The Infrastructure Manger is responsible for maintaining a suitably secure and robust operating environment for Client sites and administrative interfaces.

The Responsible Director is responsible for ensuring that sensitive data handled by us is managed appropriately. All staff (and their operational managers) are responsible for their individual actions and to act responsibly with data.

4.1. Policy review

Each operational manger is responsible for reviewing their own area of responsibility, if necessary in conjunction with other managers.

This policy is subject to a minimum of an annual review by the Infrastructure Manager. The Responsible Director will be consulted and approve all changes to ensure that controls are designed to maintain relevance and effectiveness.

4.2. Risk management and Electronic Security Incidents

Where an electronic security incident is suspected, then the relevant operational manager should report the matter to the Infrastructure Manager.

Where a staff member is concerned about the actions of their manager, they can report the incident directly to the Responsible Director.

Electronic security incidents will be recorded and reviewed to establish the cause and subsequent actions to mitigate a repeat of the incident. The review shall be the responsibility of the Responsible Director. The subsequent actions will be the responsibility of the staff nominated to perform the actions.

4.3. Security of Third Party Access

The Infrastructure Manager will only grant third party access to our internal business or hosting network systems if authorised by the Responsible Director. The third party access will be restricted to the minimum feasible to perform the required actions and for the minimum duration.

Third parties who require access to our business IT infrastructure will be subject to a contract that defines their security, confidentiality and non-disclosure obligations with respect to data that we control or process.

4.4. Assets

The Infrastructure Manager will be responsible for defining the assets that may have access to our IT systems. Any asset provided by us to a User e.g. laptop will be the joint responsibility of the User and the Infrastructure Manager to ensure that it is used in accordance with the terms of this Electronic Information Security Policy.

4.5. Security Issues – Personnel

Controls will be deployed to reduce the risks of human error, theft, fraud, nuisance or malicious misuse of facilities.

4.5.1. Roles and access levels

The Infrastructure Manager will limit access to our networks to authorised Users.

The director responsible will ensure that proof of identification is held, together with references from previous employers.

4.5.2. Job roles

Staff handbooks and employment contracts will clearly identify security requirements and the consequences of failure to comply.

4.5.3. Personal data

All data which identifies any individual will be handled in accordance with the Data Protection Legislation. All personal details will be held securely. Data transfer to/from a third party will only be progressed if, in the opinion of the relevant manager, the transfer method will maintain data confidentiality, and is necessary.

4.6. Client Data

All data that is provided by a client will be treated as confidential as detailed in our Terms of Business.

Data will only be transferred to/from the client, if in the opinion of the relevant staff member, the data transfer can be achieved whilst maintaining the confidentiality of the data.

4.6.1. Maintenance of Confidentiality

All Users have an obligation to protect confidential information in their contract of employment/engagement.

The Responsible Director will ensure that:

- confidentiality agreements form part of the terms of employment/engagement for all Users; and
- information for all staff on electronic information security is maintained in the staff handbook.

Operational Managers shall ensure that awareness training about electronic information security forms part of staff induction programmes.

4.6.2. Users leaving employment

On termination of employment, all User accounts will be immediately disabled by the Infrastructure Manager and the Operational Manager will recover any IT equipment we have issued to the User.

4.6.3. Monitoring Users

Within the provisions of the law of England and Wales, we reserve the right to intercept and monitor communications and data.

Monitoring and recording of communications and data will be carried out in accordance with the provisions of our staff handbook and interception/monitoring of individual activity shall only take place with the prior express approval of a director.

Monitoring may be undertaken without any prior notice to the User.

5. Responding to security incidents

A security incident is any incident which:

- alters, amends, deletes or transfers data without the appropriate authority;
- may cause physical damage to our IT network;
- may adversely affect the efficiency of our IT network; and/or
- contravenes our policies, statutory or legal requirements.

5.1. Reporting Security incidents

All security incidents and/or suspected security incidents must be reported to the Infrastructure Manager and Responsible Director.

5.2. Suspected security breach

The Responsible Director will determine which staff will be responsible for the investigation and resolution of the suspected breach. The collection of evidence in relation to any suspected security breach should only be made when the personnel tasked with investigation and resolution have been authorised by the Responsible

Director.

The investigation will include any data or records deemed appropriate by the Responsible Director.

When considering authorisation to investigate, the Responsible Director shall conduct a risk assessment to establish if the suspected security breach may be connected with criminal activity, may lead to disciplinary action, financial penalties, or similar outcomes. The Responsible Director may consult with such outside agencies or seek professional advice as considered necessary.

5.3. Network isolation

At the discretion of the Infrastructure Manager, any device or data on the IT systems that may adversely impact the integrity of our IT network or potentially cause a service interruption will be isolated.

Suspension of network connectivity will remain in force until the issue has been investigated and a plan of action agreed. Subsequent reinstatement will only be permitted once the requirements of that action plan have been met, verified and authorised by the Infrastructure Manager (if not available, the Responsible Director).

6. Physical and Environmental Security

6.1. Physical security

Computer systems and networks will be protected by suitable physical, technical, procedural and environmental security controls.

File servers that hold or process Sensitive or Client data will be located in physically secured locations, dedicated for IT systems equipment.

Passwords and other authentication methods shall be used to limit physical equipment access to authorised Users.

Our networks shall be insulated from connection to the internet through a firewall.

Any connection that breaches the firewall will be specifically monitored and approved by the Infrastructure Manager for specified purposes only. If authorised, it shall be active for the minimum duration necessary and then disabled so that our IT systems are not exposed.

6.2. Asset security

Servers holding Client Data and Sensitive Data will be held in a secure environment protected by:

- Physical security
- Access control
- Temperature control
- Uninterruptible power supply (UPS)

The Infrastructure Manager will ensure the IT Infrastructure is covered by appropriate hardware and software maintenance and support.

Prior to asset disposal being undertaken, the Infrastructure Manager will ensure all data is permanently erased from storage media. Physical data destruction methods may be used in addition.

7. Controls against malicious software

The Infrastructure Manager will implement controls to check for malicious or fraudulent code being introduced to or transmitted by our IT systems.

The IT system will be protected by a multi-level approach involving firewall, router configuration, e-mail scanning, and virus and spy/malware protection on all workstations on our network.

All our workstations will have appropriate anti-virus software installed by the Infrastructure Manager, configured to update anti-virus signatures automatically. This must not be disabled by Users.

Internal business network traffic will be monitored for any activity that may indicate a potential security threat to the network.

7.1. Security and updates

The Infrastructure Manager is responsible for the day-to-day management of systems and responsible for ensuring that security patches, fixes and workarounds are applied in a timely manner to reduce vulnerabilities to devices within our network.

The Infrastructure Manager will test and evaluate patches, fixes and workarounds for suitability prior to deployment.

7.2. User activities

All workstations will be appropriately secured and operated by Users who are authorised and conversant with both this policy and their personal responsibilities for confidentiality of information displayed on screen or in printed format.

Controls will be implemented to enable the correct and secure operation of information processing facilities.

Failure to comply with the requirements of this policy will leave a User liable to disciplinary and/or possible legal action.

7.2.1. Documented operating procedure

Design, build and configuration documentation will be produced in respect of system platforms and will be held securely and access restricted to IT staff on a need to know basis.

7.2.2. Segregation of duties

Access to IT systems, data and information will only be granted based on the User role and access classification.

Segregation of duties between our business operations and client environments shall be strictly maintained.

Permanent and full access to live operating environments will be restricted to staff on role based criteria.

7.3. System planning and acceptance

7.3.1. System changes

All changes to live business systems will follow a change management process, to ensure that activities are undertaken in accordance with a change control processes. A manager will be identified with the authority and responsibility to plan and implement the change so that security and operational controls are not compromised.

7.4. Controls against malicious software

Controls will be implemented by the Infrastructure Manager to check for malicious code being introduced to our systems.

All development work undertaken by us will be subject to test prior to implementation in production and live systems.

All systems will be protected by a multi-level approach involving firewall, router configuration, e-mail scanning, and virus and spy/malware protection on all workstations on our network.

All workstations will have appropriate anti-virus software installed by the Infrastructure Manager and will be set to update anti-virus signatures automatically. Any device found to pose a threat to data or the provision of our network will be isolated from the network until the security issues are resolved. Any User deliberately causing a threat to the network i.e. by removing or interrupting protective systems will be subject to disciplinary process.

Network traffic will be monitored for any anomalous activity which may indicate a security threat to the network.

7.4.1. Virus protection

A virus protection procedure will be implemented to prevent the introduction and transmission of computer viruses from both within and outside our networks. Failure to maintain a device in a state which prevents or detects virus infection will leave the device liable to exclusion from the network until the security issue is resolved.

8. Security patches

The Infrastructure Manager will be responsible for the day-to-day management of internal systems and is responsible for ensuring that security patches, fixes and workarounds are applied in a timely manner to reduce vulnerabilities to devices within the network.

The Infrastructure Manager will be responsible for the day-to-day management of our hosting platform and is responsible for ensuring that security patches, fixes and workarounds are applied in a timely manner to reduce vulnerabilities to devices within the network.

Patches, fixes and workarounds must be tested and approved before deployment and the efficiency of the deployment to the IT network will be monitored to ensure the effective mitigation of risk due to known vulnerabilities.

9. IT storage

Backups protect electronic information from major loss or failure of system software and hardware. Backups are not designed to guard against accidental deletion or overwriting of individual User data files.

System backups for our IT systems are the responsibility of the Infrastructure Manager and will cover documented systems. The procedure will include keeping backups in secure locations. Periodic checks will be made to ensure backup media can be read and files restored.

Systems backup procedures for our client hosting platform are the responsibility of the Infrastructure Manager. The procedure will include keeping backups off site in secure storage. Periodic checks will be made to ensure backup media can be read and files restored.

Backups of Client Data of the hosting platform are taken daily. Our internal business data is backed up on schedule based on a risk assessment.

10. Network management

Controls will be implemented to achieve, maintain and control access to computer networks, including wireless LANs.

The configuration of critical routers, firewall and other network security devices will be the responsibility of, maintained by, documented and kept securely by the Infrastructure Manager and relevant authorised staff.

No IT equipment may be connected to the network without approval by the Infrastructure Manager.

Any device found to cause a network compromise will have access disabled and the User may be subject to disciplinary action.

11. Device Disposal

Removable magnetic and optical media containing will be reused or disposed of through controlled and secure means when no longer required. Redundant computer equipment will be disposed of in accordance with the Waste Electrical and Electronic (WEEE) Regulations.

12. Exchange of information with outside organisations

Requests by external bodies for the provision of electronic information from our systems will in all instances be referred to the Responsible Director for consideration and potential approval. This includes data subject access requests (made under the Data Protection Legislation) and Freedom of Information Act requests.

13. Access control

Procedures for the registration and deregistration of Users and for managing access to all information systems shall be established to ensure that all Users access rights match their

authorisations. These procedures shall be implemented only by suitably authorised staff. A periodic review will be conducted to verify User access and roles.

14. Operational Policies

Access to key business systems will be appropriately controlled and comply with the access rights of the User. Access to our business network and IT Services will be restricted according to the access classification of the User.

Our staff Users may use:

- Standard software portfolio
- Non-standard software authorised by the Infrastructure Manager
- Email, calendar
- Our business systems
- Internet

Users who have been pre-approved by the Infrastructure Manager will be granted access to the hosting platform.

Guest Users:

No access to network allowed.

14.1. User responsibilities

Users of our network must comply with the policies detailed in our staff handbook. All staff (and external contractors) have written terms and conditions that include directions for the use of IT systems and data.

Access to our systems may be withdrawn and disciplinary procedures invoked where a serious or deliberate breach of the policy is made.

15. IT System access

15.1. Access management and Administration

Users will be subject to formal verification and checking procedures as part of the recruitment process for employment.

The Infrastructure Manager operates a system of access limitation depending upon the role of the User. The level of access granted to Users will be reviewed periodically to ensure that it is appropriate and necessary.

The Responsible Director (through the HR function) will carry out appropriate background and identity checks for each staff User (to include a Disclosure and Barring Service check) to establish the bona-fides of a User. Leavers will have their access disabled immediately.

15.2. Remote access

Controls will be implemented to manage and control remote access to our IT network. Specific request and authorisation will be necessary to be granted remote access.

15.3. Mobile computing

We recognise the inherent dangers of information stored on portable computers (laptops, notebooks, tablets and smart phones) as well as removable media.

It is our policy that no sensitive data should be held on a mobile device. Failure to adhere to this basic policy could lead to disciplinary action being taken (irrespective of whether data loss occurs).

15.4. Hosting platform access

Our hosting platform requires a secure Virtual Private Network (VPN) connection to access the underlying servers and infrastructure.

VPN access is restricted based on role and authorisation by the Infrastructure manager. VPN access is immediately revoked for leavers.

15.5. Password management

Users are required to follow good security practices in the selection, use and management of their passwords and to keep them confidential.

We use industry standard password management software to maintain a registry of strong and secure passwords. All changes in staff will be informed to the Infrastructure Manager, who will disable individual access to passwords, and if appropriate, change password to prevent access.

Access to our internal systems is primarily governed by a network username and password that is issued by the Infrastructure Manager. Secondary access is controlled by the permissions allocated to the User.

System passwords that control core activities (system administrator level) are maintained by the Infrastructure Manager under strict security. System administrator passwords will be issued on the express authority of the Infrastructure Manager on a need-to-know basis and will be changed regularly, including whenever an authorised system administrator leaves employment.

15.6. Unattended User equipment

Users of our network are responsible for safeguarding data. Users are required to ensure that devices are not left logged-on when unattended and that portable equipment in their custody is not exposed to opportunistic theft, unauthorised access or observation of sensitive information.

Where available, password protected screensavers and automatic log-out mechanisms are to be used on all devices.

15.7. Monitoring systems access and use

Access to and use of our networks will be monitored by the Infrastructure Manager. In accordance with the policies set out in the staff handbook, there is no presumption of privacy for any User. Monitoring may include the inspection of communications into and out of our network.

Remote access by third party contractors to maintain and support our IT systems will be subject to appropriate monitoring and control measures defined by the Infrastructure Manager. Third Party access will only be granted where the Infrastructure Manager is

satisfied that the access is relevant and appropriate. The Infrastructure Manager will disable the remote access at the completion of the agreed task.

16. Compliance

16.1. Review

This policy will be reviewed on at least an annual basis. This review will be conducted in association with the Infrastructure Manager.

16.2. Policy Breaches

In the event of a breach of this policy, the key details of the breach will be recorded in an issue log and the actions taken to prevent a re-occurrence will also be recorded.