IT SECURITY POLICY

Version: 1.4

Author: James Hall

1. Version Control

Issue Date:	03/04/2024	Review Date:	03/04/25
Version:	1.1	Issued by:	AJC - BCC
	1.4		JAH
Approved By:		Date:	
	James Hall		03/04/24
	Ethan Jones		
Review and consultation process	Ethan Jones	April 2024	To be reviewed April 2025
Responsibility for Implementation and Training:	Ethan Jones & IT Security Committee		

2. Document Revision History

This document shall be amended by releasing a new edition of the document in its entirety. The Amendment Record Sheet below records the history and issue status of this document.

Date	Author	Reason for Revision
07/12/2016	AJC-BCC	Initial version

09/02/17	JAH-PAW	Amended version
11/04/17	JAH-PAW	Revised following ISMF
March 2024	JAH-PAW	Revised following updated legislation and advice from BccIT

3. References

Ref #	Reference	Version
1	https://www.ncsc.gov.uk/section/advice-guidance/all-topics?allTopics=true&topics=cyber%20essentials&sort=date%2Bdesc	National Cyber Security Centre – Cyber essentials guidance. Updated online. (accessed 03/0424)
2	https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted	UK data protection legislation (accessed 03/0424)

4. Table of Contents

5. Introduction

This IT security policy is a key component of People and Work's overall business management framework and provides the framework for the more detailed information security documentation including system level security policies, security guidance and procedures.

Failure to implement effective information security management controls can result in People and Work becoming exposed to a number of significant threats including (but not limited to):

- Malicious code entering the network;
- Hackers obtaining unauthorised access to systems and data;
- Unauthorised persons gaining access to confidential information;
- Data leakage;
- Compromise of confidentiality, integrity and availability of company sensitive data.

The adverse impacts potentially flowing from these risks include:

- Loss of availability of key systems and/or loss of data;
- Interruption of normal operations and resultant loss of revenue;
- Damage to People and Work's reputation and loss of confidence amongst clients, employees, partners and funders;
- Allegations of poor corporate governance resulting in adverse publicity and client or funder dissatisfaction;
- Confidential information falling into the hands of competitors and other third parties;
- Reputational damage to People and Work.

Compliance with these policies, procedures and standards is therefore required from all persons who have access to any of People and Work's IT infrastructure or information assets. This includes third parties (e.g. clients, partners and – in some cases – funders) as well as employees.

6. Objectives, Aim and Scope

Objectives

The objective of this Information Security Policy is to help preserve the confidentiality, integrity and availability of our information, based upon a risk assessment and an understanding of our tolerance for risk.

Policy Aim

The aim of this policy is to set out the rules governing the secure management of our information assets.

It will achieve this by ensuring that all members of staff are aware of and fully comply with the relevant **legislation** as described in this and other policies; ensuring an approach to security in which all members of staff fully understand their own **responsibilities**, creating and maintaining within the organisation a level of **awareness** of the need for information security as an integral part of the day to day business and **protecting** information assets under the control of the organisation.

Scope

This policy applies to all information, information systems, networks, applications and users of People and Work or supplied under contract to it.

7. Responsibilities

Ultimate responsibility for information security rests with the Director of People and Work. Employees shall be responsible for managing and implementing the policy and related procedures.

Responsibility for maintaining this Policy, the Information Risk Register and for recommending appropriate risk management measures is vested in the Director. Both the Policy and the Risk Register shall be reviewed by the Information Security Management Forum annually, or more often if appropriate and reported to the Board of Trustees annually.

Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of the information security policies applicable in their work areas, their personal responsibilities for information security and how to access advice on information security matters.

All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity: failure to do so may result in disciplinary action.

Line Managers shall be individually responsible for the security of their physical environments where information is processed or stored.

Each member of staff shall be responsible for the operational security of the information systems they use.

Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

Contracts with external parties that allow access to the organisation’s information systems shall be in place before access is allowed. These contracts shall aim to ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies.

Implementation of the Information Security Management Forum (ISMF)
People and Work shall implement an ISMF that shall meet on a regular basis and at least annually.

ISMF Terms of Reference
To take overall responsibility for Information Security Management within the Information Management System Scope. This shall include representation from:

- IT Security Manager (currently, Ethan Jones)
- Human Resources (currently, Sarah Lloyd-Jones)
- Facilities Management - BccIT
- The organisation via the Head of Research (currently, Duncan Holtom) and a Trustee.

The ISMF will:

- Define ownership and responsibility for Information Security Policy and Procedures
- Set Information Security Policy within People and Work
- Have representation on board meetings to address security issues.

8. Legislation

People and Work is required to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of People and Work, who may be held personally accountable for any breaches of information security for which they may be held responsible. People and Work shall comply with the following legislation and other legislation as appropriate:

- The Data Protection Act (1998)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- The Data Protection Act 2018[1]
- UK GDPR principles[2]

[1] https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
[2] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/ (Check out the seven principles)

9. Personnel Security

Contracts of Employment

Staff security requirements shall be addressed at the recruitment stage and all prospective staff members shall be subject to a level of security screening appropriate to their role. This shall be conducted by the HR function with advice and input from the People and Work Director. As a minimum this should include:

- Verification of identity;
- Employment history (for a minimum of the past three years);

Information security expectations of staff shall be included within appropriate job definitions and that any breach of information security controls may be considered a misdemeanour under People and Work's disciplinary policy, and which in turn might, under specific circumstances, result in dismissal.
All access rights shall be removed immediately on termination of contract.

Information Security Awareness Training

Information security awareness training shall be included in the staff induction process. Users shall be made aware of the procedures applicable to them and refreshed annually. An on-going awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

Intellectual Property Rights

The organisation shall ensure that all software is properly licensed and approved by the IT Manager and BccIT, People and Work's IT support company. Individual and People and Work IPR shall be protected at all times. Users breaching this requirement may be subject to disciplinary action.

Electronic Communication, including Social Media

The following is strictly prohibited:

- Inappropriate use of communication equipment, including, but not limited to, supporting illegal activities, obscene, pornographic and procuring or transmitting material that violates People and Work policies against discriminatory or harassment or the safeguarding of confidential orproprietary information.
- Sending Spam via e-mail, text messages, pages, instant messages, voice mail, or other forms of electronic communication in breach of copyright laws.
- Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.
- Posting the same or similar, non-business-related messages to large numbers of newsgroups (newsgroup spam).
- Use of a People and Work e-mail to engage in conduct that violates People and Work policies or guidelines. Posting to a public newsgroup, a bulletin board with a People and Work e-mail or IP address represents People and Work to the public; therefore, you must exercise good judgment to avoid misrepresenting or exceeding your authority in representing the opinion of the company.

Email

These guidelines are intended to help make the best use of electronic mail facilities. The following must be understood:

- People and Work provides electronic mail to staff to enable them to communicate effectively and efficiently with other members of staff, other companies, and partner Organizations.

When using People and Work electronic mail facilities, the following guidelines followed:

- Do check electronic mail daily to see if you have any messages.
- Do include a meaningful subject line in the message.
- Do check the address line before sending a message and check it is to the correct person.
- Do delete electronic mail messages when they are no longer required.
- Do respect the legal protections to data and software provided by copyright and licenses.
- Do take care not to express views, which could be regarded as defamatory or libellous.
- Do not print electronic mail messages unless necessary.
- Do not expect an immediate reply, the recipient might not be at their computer or could be too busy to reply straight away.
- Do not forward electronic mail messages sent personally to others, particularly newsgroups or mailing lists, without the permission of the originator.
- Do not use electronic mail for personal reasons.
- Do not send excessively large electronic mail messages or attachments.
- Do not participate in chain or pyramid messages or similar schemes.
- Do not represent yourself as another person.
- Do not use electronic mail to send or forward material that could be construed as confidential, political, obscene, threatening, offensive or libellous.

Please note the following:
All electronic mail activity is monitored and logged.
All electronic mail entering or leaving the organisation is scanned for viruses.
All the content of electronic mail is scanned for offensive material.

Social Media

Social media may be used for work purposes on condition that no sensitive or potentially sensitive material, IP or similar material is disclosed. Users must behave responsibly while using any social media whether for business or personal use, bearing in mind that they directly or indirectly represent the company. If in doubt, consult the Director or IT Manager.

Users breaching this requirement may be subject to disciplinary action. People and Work has a social media policy which must be followed by all staff, volunteers and trustees.[3]

10. Asset Management

Asset Ownership

Each information asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

Asset Records and Management

An accurate record of business information assets, including acquisition, ownership, modification and disposal shall be maintained. Sensitive material such as licenced software and sensitive data shall be removed from hardware before disposal.

Removable media

Official removable media shall be provided centrally, and its use recorded (e.g. serial number, date, issued to, returned). Where indicated by a risk assessment, systems should be prevented from using removable media. Use of personal removable media in work information systems (e.g. USB sticks, CD, DVD and personal devices for the purposes of charging etc.) is forbidden unless approved by the IT Manager and, if used, all removable media must be encrypted.

Removable media from external sources

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of the IT Manager before they may be used on business systems. Such media must also be fully virus checked before being used on the organisation’s equipment. Users breaching this requirement may be subject to disciplinary action.

Mobile devices (e.g. phones, tablets, laptops etc.)

Use of mobile devices for work purposes (privately or owned by People and Work) requires the approval of the IT Manager before they may be used.

Such devices must at a minimum:

- have anti-malware software installed and updated daily
- have pin, password or other authentication installed
- have manufacturer-supplied updates applied within 14 days of release
- be encrypted wherever possible
- be capable of being remotely tracked and wiped.

Users must inform the IT Manager or the Director immediately if the device is lost or stolen and the device must be subsequently completely wiped.

[3] https://peopleandwork.org.uk/wp-content/uploads/2017/01/Social-Media-Policy.pdf

Sensitive Information Assets

People and Work shall identify particularly valuable or sensitive information assets, based upon the results of a risk assessment. The classification **SENSITIVE** shall be marked on all such material (in document and electronic form) and shall be held securely at all times. They shall not be left unattended at any time in any place where unauthorised persons might gain access to them. They should be transported securely in sealed packaging or locked containers. Data in electronic form shall be encrypted in transit. **SENSITIVE** shall cover information that the disclosure of which is likely to:

- adversely affect the reputation of the organisation or its staff or cause substantial distress to individuals;
- make it more difficult to maintain the operational effectiveness of the organisation ;
- cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organisations;
- prejudice the investigation, or facilitate the commission of crime or other illegal activity;
- breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies;
- breach statutory restrictions on disclosure of information;
- Disadvantage the organisation in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.

Information which has significant value to People and Work, and unauthorised disclosure or dissemination would result in severe financial or reputational damage should be given the higher classification of **CONFIDENTIAL**.

11. Access Control Management

Users are given sufficient rights to all systems to enable them to perform their job functions. The principles regarding access to all People and Work systems are:

- User rights are kept to a minimum at all times.
- Users requiring access to systems must make a written request to the IT manager.
- The systems administrators will be responsible for maintaining the data integrity of the end user data and for determining end-user access rights.
- Usernames and passwords are not to be shared by users. (See below for password policy)
- Intruder detection is implemented where possible. The user account is locked after three incorrect attempts.
- Where possible Multi-Factor Authentication (MFA) is enabled & enforced on any public facing service.
- User account requests will be subject to proper justification, provisioning and an approvals process, and assigned to named individuals.
- User accounts will be removed or disabled when no longer required.
- Elevated or special access privileges, such as system administrator accounts, will be restricted to a limited number of authorised individuals and these access privileges will be reviewed at least quarterly.

Physical Access

Only authorised personnel who have a justified and approved need shall be given access to restricted areas containing information systems or stored data.

Password Policy

Passwords are an important aspect of computer security. A poorly chosen password may result in
unauthorised access and/or exploitation of People and Work resources. All users, with access to People and Work systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

Policy

- All system-level passwords (e.g., root, Office 365 Administrator, application administration accounts, etc.) must be changed when appropriate.
- All user-level and system-level passwords must conform to the guidelines described below.

- **Guidelines**
- All People and Work staff should be aware of how to select strong passwords.
- Characteristics of strong passwords include, but are not limited to, the following:
- Lower case characters
- Upper case characters
- Numbers
- Punctuation
- “Special” characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc.)
- Contain at least eight alphanumeric characters.
- Where possible, passwords should contain at least three of these characteristics.
- Try to create passwords that are easily remembered. An excellent way to do this is to consider using a “pass-phrase” as opposed to a password. For instance, “Master Volume Switch 99$” is both easy to remember and highly secure. Note: Do not use any of these examples as passwords!

- **Password Protection Standards**
- Always use different passwords for People and Work accounts from other non-People and Work access (e.g., personal email account, bank account, benefits, etc.).
- Avoid using ‘personal’ passwords in the ‘business’ environment.
- Do not share People and Work passwords with anyone, including administrative assistants.

- All passwords are to be treated as sensitive, confidential People and Work information.
- Passwords should never be written down or stored on-line without encryption.
- Do not reveal a password in email, chat, or other electronic communication. (passwords from BccIT will be sent via encrypted email if necessary – currently Barracuda)
- Do not speak about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name")
- Do not reveal a password on questionnaires or security forms.
- If someone demands a password, refer them to this document and direct them to the IT manager or BccIT.
- If an account or password compromise is suspected, report the incident to the IT Manager and Director of People and Work who will liaise with BccIT.

Boundary Gateways and Firewalls

People and Work has endeavoured to maintain boundary security through the use of a firewall. The integrity of this firewall is maintained by adhering to the following rules:

- All default usernames/passwords on boundary devices have been changed and a strong password has been implemented, please see password policy statement.
- All open ports and services on each firewall have been subject to justification and approval by an appropriately qualified and authorised business representative.
- All commonly attacked and vulnerable services (such as Server Message Block (SMB) NetBIOSm tftp, RPC, rlogin, rsh, rexec) have been disabled or blocked by default at the boundary firewalls.
- All firewall rules that are no longer required are to be removed or disabled in a timely manner.
- All unnecessary remote administrative interfaces have been disabled.

Application Access

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on a current licence from the supplier.

Hardware Access

Where indicated by a risk assessment, hardware should be authenticated by MAC address on the network.

System Perimeter access

The boundary between the business systems and the Internet or other non-trusted networks shall be protected by a firewall, which shall be configured to meet the threat and continuously monitored.

Monitoring System Access and Use

An audit trail of system access and data use by staff shall be maintained by BccIT wherever practical and reviewed on a regular basis.

People & Work reserves the right to monitor systems or communications activity where it suspects that there has been a breach of policy in accordance with the Regulation of Investigatory Powers Act (2000).

12. Computer and Network Procedures

Management

Management of computers and networks shall be controlled through standard documented procedures that have been authorised by BccIT and the IT Manager.

Maintenance

Systems hardware, firmware and software shall be updated in accordance with the suppliers' recommendations as approved by the IT Manager.

Patch Management

All software installed on computers and network devices is to be fully licensed and supported by the vendor.

All security patches and updates are to be applied within 14 days of release.

Accreditation

The organisation shall ensure that all new and modified information systems, applications and networks include security provisions, are correctly sized, identify the security requirements, are compatible with existing systems according to an established systems architecture (as required) and are approved by the IT Manager before they commence operation.

System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the IT Manager and BccIT.

Local Data Storage

Data stored on the business devices shall be backed up regularly and restores tested at appropriate intervals (at least weekly). The default storage location for all business-related data should be on the secure online business server (currently Microsoft 365).

Encryption Policy

The need for encryption has increased in recent years. People and Work recognises the need to secure
its data, protect its staff and clients and have strict control over data in transit. This policy describes
measures for the protection of all personal data and/or business-critical information from unauthorised

access, disclosure or loss using data encryption and sets out the People and Work policy for the use of
encryption for organisational purposes.
Encryption techniques are deployed by People and Work to enhance the confidentiality, integrity, and
availability of data held, and also to prevent unauthorised disclosure of People and Work information
assets and disruption to People and Work business so safeguarding the reputation of People and Work.
People and Work has a responsibility to provide appropriate secure storage mechanisms for those staff
required to transport client data and/or business-critical information on Mobile Data Devices.

Policy Statement

The encryption process is managed and supported by technical staff and non-IT staff must not attempt
to modify, disable or tamper with the process in any way. In cases where encryption is clearly not
working, or where there is any doubt, the user should immediately seek advice through IT staff or
through a designated third-party support company (currently, BccIT).

Mobile Data Devices

All People and Work laptops must have approved device encryption software installed before it is
supplied to the user and the hard disk must be fully encrypted at all times. It is the user's responsibility
to respond to any error messages and immediately report issues to the relevant technical contacts,
thereby ensuring the encryption mechanism is operating correctly.

Email

Many staff use email to transfer information. Such exchanges must be undertaken securely as detailed
in the IT and Social Policies. All confidential client data and/or business critical information that's deemed appropriate by Senior Management for transmission as an email attachment can be encrypted. This will be achieved using content encryption and it is the user's responsibility to ensure that this happens. Email encryption is available through Office 365 using the Outlook client. It is acceptable to access People and Work email from external devices for business purposes. When accessing email externally, for example from a home PC, Outlook Web Access must be used and the downloading of Personal Data and/or Business Critical Information to the local device is prohibited.

Loss or Theft of Devices

Staff must immediately report the loss or theft of mobile data devices/smartphones to their Line
Manager. Any devices returned to People and Work following a loss or theft must be reported to IT Staff and
returned as instructed for checking and reconfiguration, as necessary. Staff must return equipment on demand and assist in the implementation of audit, patches and security software if and when this becomes necessary.
Staff failing to adhere to any of the conditions herein may face disciplinary action and People and Work
reserves the right to disable user accounts, deny access, impound equipment and remove the right to
use mobile data devices.

User Awareness

Users shall be made aware of their responsibilities in the prevention of unauthorised access to
People and Work information resources, including, but not limited to:

- The need to encrypt all sensitive or critical data which is to be transported or transmitted;
- That suspicious activity is to be reported immediately to a Director.

External Cloud Services

People and Work has selected to implement the Microsoft Office 365 and cloud computing solutions as a method of delivering Information and Communication Technology (ICT) services to its users. Using Software as a Service (SaaS) (i.e. Microsoft 365 - Exchange Online, Sharepoint) means that People and Work has no on-premises servers to identify, with Cloud Services being the primary means for Email & File Services. It is imperative the Cloud provider:

- ensures 99.9% uptime of cloud services (with sufficient data centre resilience to relocate)
- data is stored securely and protected from compromise
- People and Work must ensure:
- users upload and save only business-related files to the cloud
- users do not exceed the storage allowance agreed with the Cloud Provider
- all files and data stored in the Cloud have an appropriate Cloud Backup solution in operation (currently managed via BccIT)
- a periodic restore exercise of their data is performed to ensure the quality and integrity of the backup data.

Legal & Policy Basis

The procurement, evaluation and use of cloud services must adhere to the legislation in force;

- Copyright and Related Rights Acts 2007

- General Data Protection Regulations 2018
- Freedom of Information Act 1997 and 2003

Control Statements

Legal obligations relating to information security and other aspects of implementing and operating outsourced services, such as commercial and reputational risk, will be evaluated and managed through the use of risk assessments and contractual agreements.
A formal procurement process, including a risk assessment and review of proposed contractual terms and conditions, must be undertaken to assess whether a People and Work service can be supplied via cloud computing services. Consideration should be given to existing procedures around IT project management and risk assessment.
Advice on the information security aspects of cloud computing can be provided by the Information Security team at BccIT where required.

Cloud Storage

The use of personal cloud storage for People and Work business – such as Dropbox, Google Drive, and Microsoft OneDrive – is not permitted.

Assessment of Cloud Solutions

Cloud computing solutions will be evaluated on a case-by-case basis against the People and Work information security policies, procedures and guidelines as well as established good practice, such as the National Cyber Security Centre Cloud Security Principles[4].

Data in transit protection - User data transiting networks should be adequately protected against tampering and eavesdropping via a combination of network protection and encryption. If this principle is not implemented, then the integrity or confidentiality of the data may be compromised whilst in transit.

Asset protection and resilience - User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure. If this principle is not implemented, inappropriately protected consumer data could be compromised which may result in legal and regulatory sanction or reputational damage.

Separation between users - A malicious or compromised user of the service should not be able to affect the service or data of another. If this principle is not implemented, service providers cannot prevent a consumer of the service affecting the confidentiality or integrity of other consumer's data or service.

Governance framework - The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. If this principle is not implemented, any procedural, personnel, physical and technical controls in place will not remain effective when responding to changes in the

[4] Cf. https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

service and to threat and technology developments. Any technical controls deployed outside of this framework will be fundamentally undermined.

Operational security - The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes. If this principle is not implemented, the service cannot be operated and managed securely in order to impede, detect or prevent attacks against it.

Personal security - Where service provider personnel have access to your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel. If this principle is not implemented, the likelihood of accidental or malicious compromise or consumer data by service provider personnel is increased.

Secure development - Services should be designed and developed to identify and mitigate threats to their security. If this principle is not implemented, services may be vulnerable to security issues which could compromise consumer data, cause loss of service or enable other malicious activity.

Supply chain security - The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement. If this principle is not implemented, it is possible that supply chain compromise can undermine the security of the service and affect the implementation of other security principles.

Secure user management - Your provider should make the tools available for you to securely manage your use of their service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorised access and alteration of your resources, applications and data. If this principle is not implemented, unauthorised people may be able to access and alter consumer's resources, applications and data.

Identity and authentication - All access to service interfaces should be constrained to authenticated and authorised individuals. If this principle is not implemented, unauthorised changes to a consumer's service, theft or modification of data, or denial of service may occur.11. External interface protection - All external or less trusted interfaces of the service should be identified and appropriately defended. If this principle is not implemented interfaces could be subverted by attackers in order to gain access to the service or data within it.

Secure service administration - Systems used for administration of a cloud service will have highly privileged access to that service. If this principle is not implemented, an attacker may have the means to bypass security controls and steal or manipulate large volumes of data.

Audit information for users – Consumers should be provided with the audit records they need to monitor access to their service and data held within it. If this principle is not implemented, a consumer will not be able to detect and respond to inappropriate or malicious use of their service or data within reasonable timescales.

Secure use of services - The security of cloud services and the data held within them can be undermined if you use the service poorly. Consequently, you will have certain responsibilities when using the service for your data to be adequately protected. If this principle is not implemented, the security of cloud services and data held within them can be undermined by poor use of the service by consumers. Cloud computing solutions must deliver the same or better levels of service as an in-house solution to ensure business continuity, in line with the requirements of the business service being delivered. Consideration should be given to the nature of the information being stored in the cloud solution, in-line with People and Work Information Security Procedure.

13. Protection from Malicious Software

The organisation shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software or other active code on the organisation's property without permission from the IT Manager. Users breaching this requirement may be subject to disciplinary action. All Malware Protection Software will have all engine updates applied, and this application is to be strictly adhered to. Daily Malware scans will be implemented using the company's anti-malware software.

14. Information Security Incidents and Weaknesses

All breaches of this Policy and other information security incidents or suspected weaknesses are to be reported to the IT Manager immediately. Information security incidents shall be logged and investigated to establish their cause and impacts with a view to avoiding similar events. If required as a result of an incident, data will be isolated to facilitate forensic examination.

15. Business Continuity and Disaster Recovery Plans

The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

16. Reporting

The IT Manager shall keep the organisation informed of the information security status by means of regular reports to the Board of Trustees.

Policy approved by:

Signature J. A. Hall

Date 03/04/2024