Title:	**Information Security**			**Doc No:**	IS-POL-001
Author:	M Roberts			**Rev:**	0
Owner:	M Roberts	**Approved:**	C Barley	**Date:**	06/06/2018

Information Security Policy

Foreword to the Information Security Policy

The current climate is often referred to as the "information age". We have seen a massive change in the way humans generate, store and exchange information. It has also profoundly altered the terms by which we interact with each other, not just as individuals, but also within and between institutions, societies and nations. We have accrued great benefits from this new climate, but it brings with it profound challenges in the areas of security and privacy, which have been reflected in the growth of legislation around the globe concerning the holding of information.

Our organisation has an ethical, legal and professional duty to ensure that the information we hold conforms to the principles of confidentiality, integrity and availability. We must ensure that the information we hold or are responsible for is safeguarded where necessary against inappropriate disclosure, is accurate, timely and attributable; and is available to those who should be able to access it.

The Information Security Policy below provides the framework by which we take account of these principles. Its primary purpose is to enable everyone to understand both their legal and ethical responsibilities concerning information, and empower them to collect, use, store and distribute it in appropriate ways.

1 Introduction

The confidentiality, integrity and availability of information, in all its forms, are critical to the on-going functioning of our organisation. Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for our organisation to recover.

This information security policy outlines our approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of the organisations information systems. Supporting policies, codes of practices, procedures and guidelines provide further detail.

We are committed to a robust implementation of Information Security Management. It aims to ensure the appropriate confidentiality, integrity and availability of data. The principles defined in this policy will be applied to all of the physical and electronic information assets for which we are responsible.

We are specifically committed to preserving the confidentiality, integrity and availability of documentation and data supplied by, generated by and held on behalf of third parties pursuant to the carrying out of work agreed by contract in accordance with the requirements of data security standard ISO27001.

1.1 Objectives

The objectives of this policy are to:

1. Provide a framework for establishing suitable levels of information security for all our information systems and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems.
    a. This explicitly includes any ISO27001 certified Information Security Management Systems we may run
    b. The resources required to manage such systems will be made available
    c. Continuous improvement of any ISMS will be undertaken.
2. Make certain that users are aware of and comply with all current and relevant UK and EU legislation,
3. Provide the principles by which a safe and secure information systems working environment can be established for staff, students and any other authorised users.
4. Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.
5. Protect us from liability or damage through the misuse of IT facilities
6. Respond to changes in the context of the organisation as appropriate, initiating a cycle of continuous improvement.

1.2 Scope

This policy is applicable to, and will be communicated to. All staff, students, other members of the organisation and third parties who interact with information held by us and the information systems used to store and process it.

This includes, but is not limited to: any system or data attached to our data or telephone networks, systems managed by us, mobile devices used to connect to our network or hold our data, data over which we are the data controller and data processor, electronic communications sent from us.

2 Policy

2.1 Information security principles

The following information security principles provide overarching governance for the security and management of information at our organisation.

1. Information should be classified according to an appropriate level of confidentiality, integrity and availability and in accordance with legislative, regulatory and contractual requirements
2. Staff with particular responsibilities for information must ensure the classification of that information, must handle that information in accordance with its classification level, and must abide by any contractual requirements, policies, procedures or systems for meeting those requirements.
3. All users covered by the scope of this policy must handle information appropriately and in accordance with its classification level.
4. Information should be both secure and available to those with legitimate need for access in accordance with its classification.
5. Information will be protected against unauthorised access or processing in accordance with its classification level
6. Breaches of this policy must be reported
7. Information security provision and the policies that guide it will be regularly reviewed, including through the use of annual internal audits.

2.2 Legal and Regulatory Obligations

Our organisation has a responsibility to abide by and adhere to all current UK and EU legislation as well as a variety of regulatory and contractual requirements.

A non-exhaustive summary of the legislative and regulatory and contractual obligations that contribute to the form and content of this policy.

Related policies will detail other applicable legislative requirements or provide further detail on the obligations arising from the legislation summarised below.

2.3 Information Classification

The following table provides a summary of the information classification levels that have been adopted by our organisation and underpin the 8 principles of information security defined in this policy.

These classification levels explicitly incorporate the General Data Protection Regulation's definitions of Personal Data and Special Categories of Personal Data.

Security Level	Definition	Examples
1. Confidential	Normally accessible only to specified members of the organisation. Should be held in an encrypted state.	GDPR – defined Special Categories of personal data (racial/ethnic origin, political opinion, religious beliefs, trade union membership, physical/mental health condition, sexual life, criminal record)
2. Restricted	Normally accessible only to specified members of the organisation	GDPR – defined Personal Data (information that identifies individuals including home/work address, age, telephone number, schools attended) Draft reports, papers and minutes
3. Internal Use	Normally accessible only to members of staff	Internal correspondence Final working group papers and minutes Committee papers
4. Public	Accessible to all members of the public	Annual accounts Minutes of statutory and other formal committees Pay scales etc. Information of the organisation website

2.4 Suppliers

All suppliers will abide by the organisations Information Security Policy, or otherwise be able to demonstrate corporate security policies providing equivalent assurance. This includes:

- When accessing or processing our assets, whether on site or remotely
- When subcontracting to other suppliers

2.5 Cloud Providers

Under GDPR, a breach of personal data can lead to a fine of up to 4% of global turnover. Where our organisation uses cloud services. Our organisation retains responsibility as the data controller for any data it puts into the service, and can consequently be fined for any data breach, even if this is the fault of the cloud service provider. Our organisation will bear responsibility for contacting Information Commissioners Office concerning the breach as well as any affected individual. It will also be exposed to any lawsuit for damages as a result of the breach. It is extremely important, as a consequence, that our organisation is able to judge the appropriateness of a Cloud service provider's information security provision. This leads to the following stipulations:

- All providers of cloud services to our organisation must respond to cloud services assurances questionnaire prior to a service being commissioned. In order for us to understand the provider's information security provision
- Cloud services used to process personal data will be expected to have ISO270001 certification, with adherence to the standard considered the best way of a supplier proving that it has met the GDPR principle of privacy by design, and that it has considered information security throughout its service model.
- Any request for expectations will be considered by the Risk Manager.

2.6 Compliance, Policy Awareness and Disciplinary Procedures

Any security breach of our information systems could lead to the possible loss of confidentiality, integrity and availability of personal or other confidential data stored on these information systems. The loss or breach of confidentiality of personal data is an infringement of the General Data Protection Regulation, contravenes our Data Protection Policy, and may result in criminal civil action against our organisation.

The loss or breach of confidentiality or contractually assured information may result in the loss of business, financial penalties or criminal or civil action against our organisation. Therefore it is critical that all users of the organisations information systems adhere to the Information Security Policy and its supporting policies.

All current staff, students and other authorised users will be informed of the existence of this policy and the availability of supporting policies, codes of practice and guidance's.

Any security breach will be handled in accordance with all relevant organisational policies.

2.7 Incident Handling

In a member of staff or student, is aware of an information security incident then they must report it to the Directors.

Breaches of personal data will be reported to the information Commissioner's Office by the Directors.

2.8 Review and Development

This policy shall be reviewed by the Directors and updated regularly to ensure that it remains appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.

Additional regulations may be created to cover specific areas.

Appendix A: Summary of supporting legislation

The Computer misuse Act 1990

Defines offence in relation to the misuse of computers as:

- Unauthorised access to computer material
- Unauthorised access with intent to commit or facilitate commission of further offences
- Unauthorised modification of computer material

The Freedom of Information Act 2000

The Freedom of Information Act 2000 (FOIA2000) is a general right of public access to all types of recorded information held by public authorities in order to promote a culture of openness and accountability

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 regulates the powers of public bodies to carry out surveillance and investigation. It covers the interception and use of communications data and can be invoked in the cases of national security, and for the purpose of detecting crime, preventing disorder, public safety and protecting public health.

Defamation Act 1996

Defamation is a false accusation of an offence or malicious misrepresentation of someone's words or actions. The defamation laws exist to protect a person or an organisation's reputation from harm.

Obscene Publications Act 1959 and 1964

The law makes it an offence to publish, whether for gain or not, any content whose effect will tend to "deprave or corrupt " those likely to read, see or hear the matter contained or embodied in it. This could include images of extreme sexual activity such as bestiality, necrophilia, rape or torture.

Protection of Children Act 1978, Criminal Justice Act 1988, Criminal Justice and Immigration Act 2008

The Protection of Children Act 1978 prevent the exploitation of children by making indecent photographs of them and penalises the distribution and showing of such indecent photographs. Organisations must take appropriate steps to prevent such illegal activities by their workers using their digital systems and networks.

The definition of photographs' include data stored on a computer disc or by other electronic means which is capable of conversion into an image.

It is an offence for a person to distribute or show such indecent photographs, or to possess such indecent photographs, with a view to their being distributed or shown by himself or others.

Section 160of the Criminal Justice Act 1988 makes the simple possession of indecent photographs of children an offence. Making an indecent image of a child is a serious arrestable offence carrying a maximum sentence of 10 years imprisonment.

Terrorism Act 2006

The Terrorism Act 2006 makes it an offence to write, publish or circulate any material that could be seen by any one or more of the persons to whom it has or may become available, as a direct or indirect encouragement or other inducement to the commission, preparation or instigation of acts of terrorism.

It also prohibits the writing, publication or circulation of information which is likely to be useful to any one or more persons in the commission or preparation of terrorist acts or is in a form or context in which it is likely to be understood by any one or more of those persons as being wholly or mainly for the purpose of being so useful.

In addition, it prohibits the glorification of the commission or preparation (whether in the past, in the future or generally) of terrorist acts or such offences; and the suggestion that what is being glorified is being glorified as conduct that should be emulated in existing circumstances.

General Data Protection Regulation

The GDPR will apply in the UK from 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect implementation of the GDPR. The GDPR reinforces and extends data subjects' rights as laid out in the Data Protection Act 1998, and provides additional stipulations around accountability and governance, breach notification and transfer of data. It also extends the maximum penalties liable due ti a data breach, from £500,000 to 4% of global turnover.

The GDPR requires our organisation to maintain an Information Asset register, to ensure where personal data is voluntarily gathered people are required to explicitly opt in, and can also easily opt-out. It requires data breaches to be reported to the Information Commissioner's Office within 72Hrs of our organisation becoming aware of their existence.