Creative Process Digital
Information Security Policy

Introduction

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

This information security policy outlines Creative Process Digital's approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of the information systems. Supporting policies, codes of practice, procedures and guidelines provide further details.

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

Creative Process Digital is 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 security data standards.

Purpose

The primary purposes of this policy are to:
1. Ensure the protection of all information systems (including but not limited to all computers, mobile devices, networking equipment, software and data) and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems.

2. Make certain that users are aware of and comply with all current and relevant UK and EU legislation.

3. Provide a safe and secure information systems working environment 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 Creative Process from liability or damage through the misuse of its IT facilities.

6. Respond to feedback and update as appropriate, initiating a cycle of continuous improvement.

Scope

This policy is applicable to, and will be communicated to, all staff, students and third parties who interact with information held by Creative Process Digital and the information systems used to store and process it. This includes, but is not limited to, any systems or data attached to the Creative Process Digital data or telephone networks, systems managed by Creative Process Digital, mobile devices used to connect to Creative Process Digital networks or hold Creative Process data, data over which Creative Process Digital holds the intellectual property rights, data over which Creative Process Digital is the data owner or data custodian, communications sent to or from the Creative Process Digital.

Definitions

Creative Process Data, for the purposes of this policy, is data owned, processed or held by Creative Process Digital, whether primary or secondary, irrespective of storage location.

Policy

Information security principles

The following information security principles provide overarching governance for the security and management of information at Creative Process Digital.

1. Staff with responsibilities for information (see *Section Responsibilities*) are responsible for ensuring the classification of that information; for handling that information in accordance with its classification level; and for any policies, procedures or systems for meeting those responsibilities.

2. All users covered by the scope of this policy (see *Section Scope*) must handle information appropriately and in accordance with its classification level.

3. Information should be both secure and available to those with a legitimate need for access in accordance with its classification level. a. On this basis, access to information will be on the basis of *least privilege* and *need to know*.

4. Information will be protected against unauthorized access and processing in accordance with its classification level.

5. Breaches of this policy must be reported (see Sections *Compliance* and *Incident Handling*).

Legal & Regulatory Obligations

Creative Process Digital 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 legislation and regulatory and contractual obligations that contribute to the form and content of this policy is provided in *Appendix A*.

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

Compliance, Policy Awareness and Disciplinary Procedures

Any security breach of 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 Data Protection Act (1998), contravenes Creative Process Digital's Data Protection Policy, and may result in criminal or civil action against Creative Process Digital.

The loss or breach of confidentiality of contractually assured information may result in the loss of business, financial penalties or criminal or civil action against Creative Process Digital. Therefore, it is crucial that all users of the 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 guidelines.

Incident Handling
If a member of the company (staff or student) is aware of an information security incident, then they must report it to the CEO at stephen@creativeprocessdigital.com or telephone 01273 232 273.
If necessary, members can also use the Whistle Blowing Policy.

Supporting Policies, Codes of Practice, Procedures and Guidelines
Supporting policies have been developed to strengthen and reinforce this policy statement. These, along with associated codes of practice, procedures and guidelines are published together and are available for viewing on the Creative Process Digital website.

All staff, students and any third parties authorised to access the network or computing facilities are required to familiarise themselves with these supporting documents and to adhere to them in the working environment.

Review and Development
This policy, and its subsidiaries, shall be reviewed by the Senior Management Team and updated regularly to ensure that they remain 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. It shall oversee the creation of information security and subsidiary policies.

Responsibilities

Members of Creative Process Digital:

All members of Creative Process Digital, associates, agency staff working for Creative Process Digital, third parties and collaborators on Creative Process Digital projects will be users of Creative Process Digital information. This carries with it the responsibility to abide by this policy and its principles and relevant legislation, supporting policies, procedures and guidance. No individual should be able to access information to which they do not have a legitimate access right. Notwithstanding systems in place to prevent this, no individual should knowingly contravene this policy, nor allow others to do so. To report policy contraventions, please see *Section Incident Handling*

Data Owners/Guardians:

Many members of Creative Process Digital will have specific or overarching responsibilities for preserving the confidentiality, integrity and availability of information. These include:

Principal Investigators/Project administrators:

Responsible for the security of information produced, provided or held in the course of carrying out research, consultancy or knowledge transfer activities. This includes ensuring that data is appropriately stored, that the risks to data are appropriately understood and either mitigated or explicitly accepted, that the correct access rights have been put in place, with data only accessible to the right people, and ensuring there are appropriate backup, retention, disaster recovery and disposal mechanisms in place.

***Chief Executive/Directors*:**

Responsible for the information systems (e.g. HR/Registry/Finance) both manual and electronic that support Creative Process Digital's work. Responsibilities as above (for *Principal Investigators/Project administrators*).

***Managers/Tutors/Assessors/Internal Quality Assurers*:**

Responsible for specific area of Creative Process Digital work, including all the supporting information and documentation that may include working documents/ contracts/ staff or student information.

Appendix A: Summary of relevant legislation

The Computer Misuse Act 1990

Defines offences in relation to the misuse of computers as:
1. Unauthorised access to computer material.
2. Unauthorised access with intent to commit or facilitate commission of further offences.
3. Unauthorised modification of computer material.

Data Protection Act 2018

Provides a safeguard for personal privacy in relation to computerised or other systematically filed information; it regulates the use of *personal data* meaning information about living human beings. It is an offence to process personal data except where they are:
1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept for longer than is necessary
6. Processed in line with your rights
7. Secure
8. Not transferred to countries outside the EEA without adequate safeguards

Creative Process Digital has a Data Protection Policy which further governs the use of personal data.

The 'UK GDPR' is part of Data Protection Act 2018. It is for DPOs and others who have day-to-day responsibility for data protection. It explains the general data protection regime that applies to most UK businesses and organisations. It covers the UK General Data Protection Regulation (UK GDPR), tailored by the Data Protection Act 2018.

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 purposes of detecting crime, preventing disorder, public safety and protecting public health.

Defamation Act 1996
“Defamation is a false accusation of an offence or a 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 and 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 *prevents 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 160 of the Criminal Justice Act 1988 made 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. Note: The term "make" includes downloading images from the Internet and storing or printing them out.

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.

Counter-Terrorism and Security Act 2015 – Statutory Guidance
The statutory guidance accompanying the Counter-Terrorism and Security Act 2015 requires Creative Process to have "due regard to the need to prevent people from being drawn into terrorism."

The Act imposes certain duties under the *Prevent* programme, which is aimed at responding to "the ideological challenge we face from terrorism and aspects of extremism, and the threat we face from those who promote these views."

The Prevent programme also aims to provide "practical help to prevent people from being drawn into terrorism and ensure they are given appropriate advice and support". Creative Process Digital must balance its existing legal commitments to uphold academic freedom and freedom of speech within the law against the new Prevent duty and seek to ensure that its IT facilities are not used to draw people into terrorism.