Data & Information Protection Policy

ViewfinderUK CIC

Data & Information Protection Policy

Pretty Hate Project Productions CIC

2017

(Updated 17.03.17)

Document Control

Organisation	Viewfinderuk CIC
Title	Data & Information Protection Policy
Author	Matthew Ford
Filename	VF CIC DATA POLICY
Owner	Matthew Ford- Director (VF CIC)
Subject	Data and information policy
Review date	17.03.18

Table of Contents

Policy Statement

VIEWFINDERUK CIC (Hereby referred to as VF CIC) will ensure the protection of all information assets within the custody of the Business.

High standards of confidentiality, integrity and availability of information will be maintained at all times.

Purpose

Data and Information is a major asset that VF CIC has a responsibility and requirement to protect.

Protecting information and data assets is not simply limited to covering the stocks of information (electronic data or paper records) that the Organisation maintains. It also addresses the people that use them, the processes they follow and the physical computer equipment used to access them.

This Data & Information Protection Policy addresses all these areas to ensure that high confidentiality, quality and availability standards of information are maintained.

The following policy details the basic requirements and responsibilities for the proper management of information assets at VF CIC. The policy specifies the means of information handling and transfer within the Business.

Scope

This Data & Information Protection Policy applies to all the systems, people and business processes that make up the Business's information systems. This includes all Executives, Committees, Departments, Partners, Employees, contractual third parties and agents of the Organisation who have access to Information Systems or information used for VF CIC purposes.

Definition

This policy should be applied whenever Business Information Systems or information is used. Information can take many forms and includes, but is not limited to, the following:

- Hard copy data printed or written on paper.
- Data stored electronically.
- Communications sent by post / courier or using electronic means.
- Stored tape or video.
- Speech.

Risks

VF CIC recognises that there are risks associated with users accessing and handling information in order to conduct official business.

This policy aims to mitigate the following risks:

- The non-reporting of information security incidents and/or information that there is a legal obligation to report
- Inadequate and/or incomplete destruction of personal and/or sensitive data where required
- The loss of direct control of user access to information systems and facilities etc.
- The unauthorised sharing of data and/or information with unauthorised other parties

Non-compliance with this policy could have a significant effect on the efficient operation of the organisation and may result in financial loss and an inability to provide necessary services to our customers.

Applying the Policy

For information on how to apply this policy, readers are advised to refer to Appendix 1.

Policy Compliance

If any user is found to have breached this policy, they may be subject to VF CIC's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from MATTHEW FORD [director VF CIC]

Policy Governance

The following table identifies who within VF CIC is Accountable and responsible with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.

Responsible	Matthew Ford- Director
Accountable	Matthew Ford- Director

Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by MATTHEW FORD.

References

The following VF CIC policy documents are directly relevant to this policy, and are referenced within this document:

- Email Policy.
- Internet Acceptable Usage Policy.
- Software Policy.
- Computer and Telephone Use Policy.
- Remote Working Policy.
- Removable Media Policy.

The following VF CIC policy documents are indirectly relevant to this policy:

- IT Access Policy.
- Legal Responsibilities Policy.
- Human Resources Information Security Standards.

Key Messages

- The Business must draw up and maintain inventories of all important data and information assets.
- All data and information assets, where appropriate, must be assessed and classified by the owner in accordance with the HMG Security Policy Framework (SPF).
- Access to data and information assets, systems and services must be conditional on acceptance of the appropriate Acceptable Usage Policy.
- Users should not be allowed to access information until MATTHEW FORD- director of VF CIC is satisfied that they understand and agree the legislated responsibilities for the information that they will be handling.
- PROTECT and RESTRICTED information must not be disclosed to any other person or organisation via any insecure methods including paper based methods, fax and telephone.

Appendix 1

A1 Applying the Policy

A1.1 Information Asset Management

A1.1.1 Identifying Information Assets

The process of identifying important information assets should be sensible and pragmatic.

Important information assets will include, but are not limited to, the following:

- Computer databases.
- Data files and folders.
- Physical assets (computer equipment and accessories, PDAs, cell phones).
- Key services.
- Key people.
- Intangible assets such as reputation and brand.

A1.1.2 Personal Information

Personal information is any information about any living, identifiable individual. The business is legally responsible for it. Its storage, protection and use are governed by the Data Protection Act 1998.

A1.1.3 Assigning Asset Owners

All important data and information assets must have a nominated owner and should be accounted for. An owner must be a member of staff whose seniority is appropriate for the value of the asset they own. The owner's responsibility for the asset and the requirement for them to maintain it should be formalised and agreed. Unless otherwise stated, the owner will be MATTHEW FORD.

A1.1.4 Unclassified Information Assets

Items of data and information that have no security classification and are of limited or no practical value should not be assigned a formal owner or inventoried. Information should be destroyed if there is no legal or operational need to keep it.

A1.1.5 Information Assets with Short Term or Localised Use

For new documents that have a specific, short term localised use, the creator of the document will be the originator. This includes letters, spread sheets and reports created by staff. All staff must be informed of their responsibility for the documents they create.

A1.1.6 Corporate Information Assets

For data and information assets whose use throughout the organisation is widespread and whose origination is as a result of a group or strategic decision, a corporate owner must be designated and the responsibility clearly documented. This should be the person who has the most control over the information.

A1.1.7 Acceptable Use of Information Assets

VF CIC must document, implement and circulate Acceptable Use Policies (AUP) for information assets, systems and services. These should apply to all VF CIC Executives, Committees, Departments, Partners, Employees, contractual third parties and agents of the business and use of the system must be conditional on acceptance of the appropriate AUP. This requirement must be formally agreed and auditable.

As a minimum this will include:

- Email Policy.
- Internet Acceptable Usage Policy.
- Computer and Telephone Misuse Policy.

A1.2 Information Storage

All electronic information will be stored on centralised facilities to allow regular backups to take place.

A1.3 Disclosure of Information

A1.3.1 Sharing PROTECT or RESTRICTED Information with other Organisations

Data and information of a sensitive and/or personal nature **must not** be disclosed to any other person or organisation via any insecure method including, but not limited, to the following:

- Paper based methods.
- Fax.
- Telephone.

Where information is disclosed/shared it should only be done so in accordance with a documented Information Sharing Protocol and/or Data Exchange Agreement.

An official email legal disclaimer must be contained with any email sent. This can be found in [Name a relevant policy – but likely to be the Email Policy].

Any sharing or transfer of Council information with other organisations must comply with all Legal, Regulatory and Council Policy requirements. In particular this must be compliant with the Data Protection Act 2000, The Human Rights Act 2000 and the Common Law of Confidentiality.

END OF DOCUMENT

Data & Information Protection Policy