CONFIDENTIAL

PROCREATION

# Information Security Policy

Version: 1.2

This version issued: 01/10/22

Date approved: 01/10/22

Date for review: 01/10/23

Owner: Matt Francis, Chief Technology Officer

| | | | |
|---|---|---|---|
| Policy Title: | Data Information Security Policy | | |
| | | | |
| Issue Date: | 01.10.22 | Review Date | Periodically as necessary to meet the business needs |
| | | | |
| Version: | 1.2 | Issued by: | Matt Francis |
| | | | |
| Scope: | Procreation UK Limited | | |
| | | | |
| Associated Documentation: | | | |
| Appendices: | | | |
| Approved by: | Matt Francis | | |
| | | | |
| Review and Consultation Proces: | Regular review on date above by Matt Francis | | |
| Responsibility for Implementation and Training: | Day to day responsibility for implementation is Matt Francis<br>Day to day responsibility for training is Matt Francis | | |
| | | | |
| Revisions: | | | |
| Date: | Author: | Description: | |
| 01.10.19 | Matt Francis | 1.0 | |
| 01.10.21 | Matt Francis | 1.1 | |
| 01.10.22 | Matt Francis | 1.2 | |
| Distribution: | Stored on Tresorit private drive. | | |

## Table of Contents

Table of Contents 3

1. Introduction 4

2. Aim and Scope 4

3. Responsibilities 4

Team leaders and Team Members 4

Freelancers (and contractors) 5

Remote team members (if applicable) 5

4. Legislation 5

5. Personnel Security 6

Contracts of Employment 6

Information Security Awareness Training 6

Intellectual Property Rights 6

Social Media 6

6. Asset Management 6

Asset Ownership 6

Asset Records and Management 6

Bring Your Own Device and Mobiles (e.g. phones, tablets, laptops, etc.) 6

Removable media 7

Information Classification Policy 7

Third Party Services 8

7.  Access Management 8

7. Physical and Environmental Management 8

8. Computer and Network Procedures 8

9. Cyber Essentials 9

10. Malware Protection 9

11. Information security incidents and weaknesses 9

12. Business Continuity and Disaster Recovery Plans 9

13. Electronic Commerce 9

14. Reporting 9

15. Further Information 9

## 1. Introduction

Information security is the protection of information against accidental or malicious disclosure, modification or destruction. Information is an important, valuable asset of Procreation which must be protected and managed with care.

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

This information security policy forms the baseline of our information security management system (ISMS) and is a key component of our business framework.

The purpose of this policy is to keep all the information that pertains to Procreation as safe as we possibly can; there are elements of this policy that are explained in more detail in other, more specific policies.

## 2. Aim and Scope

The aim of this policy is to set out the rules governing the secure management of our information assets by ensuring that all team members:

- 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 the team 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.

This policy applies to all information (data), information systems, networks, applications, locations and users of Procreation services or supplied under contract to it. This also includes hardware such as laptops, mobile devices, networks and more.

## 3. Responsibilities

Ultimate responsibility for information security rests with the CTO of Procreation. They shall be responsible for managing and implementing the policy and related procedures.

Responsibility for maintaining this Policy, the Information Risk Assessment and for recommending appropriate risk management measures is vested in the CTO. Both the Policy and the Risk Assessment shall be reviewed by the CTO annually, or more often if appropriate.

### Team leaders and Team Members

Team leaders are responsible for ensuring that their permanent and temporary team members and contractors are aware of:

- The information security policies applicable in their work areas
- Their personal responsibilities for information security
- How to access advice on information security matters

All team members, freelancers and remote workers shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action, including dismissal.

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

Each team member shall be responsible for the operational security of the information systems (laptops, desktops, etc.) 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 operation before access is allowed. These contracts shall ensure that the team members or sub-contractors of the external organisation shall comply with all appropriate security policies.

### Freelancers (and contractors)

All freelancers who do not have have access (or need) to company and/or customer data do not need to undergo Procreation's onboarding or security training.

All freelancers who do have have access (or need) to company and/or customer data will be treated as temporary team members and therefore will have to undergo most of Procreation's onboarding procedure.

### Remote team members

Remote team members are categorised as individuals who work outside of our UK office. There are specific controls that affect these individuals. All remote team members should undergo Procreation's full onboarding procedure and will perform this procedure via video call. The CTO is responsible for ensuring that all remote team members have completed this procedure and results are documented in each employees Tresorit folder.

All remote team members have to comply with:

- Procreation's cyber security policy
- Procreation's data protection policy
- UK data protection laws or higher
- Local data protection laws

All software Procreation provided or recommended shall be correctly licensed for remote team members. This effects software that has access to company and/or customer data.

## 4. Legislation

Procreation is obliged 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 Procreation who may be held personally accountable for any breaches of information security for which they may be held responsible. Procreation shall comply with the following legislation and other legislation as appropriate:

- The General Data Protection Regulation (2018)
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- The Human Rights Act (1998)
- The Regulation of Investigatory Powers Act (2000)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000
- The Electronic Communications Act (2000)
- The Freedom of Information Act (2000)
- Privacy and Electronic Communications Regulations (2003)

The CTO is responsible for staying up to date with existing laws and legislation that are applicable to Procreation as well as new laws and regulations that may be applicable to Procreation. The CTO is also responsible for communicating it to team members and other stakeholders.

## 5. Personnel Security

### Contracts of Employment

- Team members security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.
- Information security expectations of team members shall be included within appropriate job definitions.
- All access rights shall be removed immediately on termination of contract.
- All company assets have to be returned immediately on termination of contract.

### Information Security Awareness Training

- Information security awareness training shall be included in the team members onboarding process.
- Team members shall be made aware of the procedures applicable to them and refreshed regularly.
- An on-going awareness programme shall be established and maintained in order to ensure that team members awareness is refreshed and updated as necessary.

### Intellectual Property Rights

The organisation shall ensure that all software is properly licensed and approved by the CTO. Individual and Procreation intellectual property rights shall be protected at all times. Team members breaching this requirement may be subject to disciplinary action.

### Social Media

Social media may be used for business purposes on condition that no sensitive or potentially sensitive material, IP or similar material is disclosed. Team members 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 CTO. Team members breaching this requirement may be subject to disciplinary action.

## 6. 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 owners shall review access rights for whom they are responsible for every 6 months.

### Asset Records and Management

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

No paper logs or records should be retained physically. All logs and records are digitally stored and require privileged access to view relevant information.

More information can be found in our Asset Register.

### Bring Your Own Device and Mobiles (e.g. phones, tablets, laptops, etc.)

Use of personal devices requires the approval of the CTO before they may be used. Furthermore, the team member needs to participate in a Mobile Device Management program, which allows Procreation to configure and secure all devices from a central place (via the Cyber Smart Cyber Essentials portal).

Use of mobile devices for business purposes (privately or business owned) requires the approval of the CTO before they may be used. Such devices must at a minimum have anti-malware software installed (for Android and Windows) and updated daily, have pin, password or other authentication installed, be encrypted and be capable of being remotely tracked and wiped. Users must inform the CTO immediately if the device is lost or stolen and the device must be completely wiped if it cannot be recovered.

### Removable media

Only company provided removable media (such as USB memory sticks and drives) shall be used to store business data and its use shall be recorded (e.g. serial number, date, issued to, returned).

Removable media of all types that contain software or data from external sources, or that has been used on external equipment, require the approval of CTO before they may be used on business systems. Such media must be scanned by anti-virus before being used.

### Information Classification Policy

Procreation shall identify particularly valuable or sensitive information assets through the use of data classification.

All team members are responsible for handling information assets in accordance with this security policy. Where possible the data classification shall be marked upon the asset itself.

All company information shall be categorised into one of the three categories in the table below based on the description and examples provided:

| Category | Description | Example |
|---|---|---|
| Public | Information which is not confidential and can be made available publicly through any channels. | • Details of products and services on the website<br>• Published company information<br>• Social media updates<br>• Press releases |
| Confidential | Information which, if lost or made available to unauthorised persons could impact the company's effectiveness, benefit competitors or cause embarrassment to the organisation and/or its partners | • Company operating procedures and policy<br>• Client contact details<br>• Company plans and financial information<br>• Basic employee information including personal data |
| Restricted | Information which, if lost or made available to unauthorised persons, could cause severe impact on the company's ability to operate or cause significant reputational damage and distress to the organisation and/or its partners.<br>This information requires the highest levels of protection of confidentiality, integrity and availability. | • Client intellectual property<br>• Data in e-commerce systems<br>• Employee salary details<br>• Any information defined as "sensitive personal data" under the GDPR |

More information can be found in the Data Classification policy.

### Third Party Services

Data is important and valuable to Procreation. We have to co-operate and use third party services to deliver our product. This includes but is not limited to:

- Marketing tools
- Communication tools
- Application and customer analytics

All these platforms store information which can include employee data, customer data, and business information. It's therefore essential that we perform due diligence and only utilize platforms we know to be secure and have been approved by the CTO.

## 7. Access Management

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

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

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.

Where indicated by a risk assessment, hardware should be authenticated by 802.1x on the network.

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 regularly monitored.

All administrative accounts have two factor authentication enabled if available. All team members have two factor authentication enabled wherever possible.

An audit trail of system access and data use by the team shall be maintained wherever practical and reviewed on a regular basis. The business reserves the right to monitor and 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).

## 7. Physical and Environmental Management

To minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards. Physical security accreditation should be applied if necessary.

Systems shall be protected from power loss by UPS if indicated by the risk assessment.

Systems requiring particular environmental operating conditions shall be maintained within optimum requirements.

## 8. Computer and Network Procedures

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

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

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 CTO before they commence operation.

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

Data stored on the business premises (if any) shall be backed up regularly and restored and tested at appropriate intervals. A backup copy should be held in a different physical location.

Where data storage, applications or other services are provided by another business (e.g. a 'cloud provider') a supplier due diligence shall be performed to ensure that the provider uses data confidentiality, integrity and availability procedures which are satisfying Procreation's needs and requirements.

All network equipment undergoes regular automatic updates and is maintained by the CTO.

Information services and systems should be segregated via subnets and VLAN's and DHCP where appropriate.

## 9. Cyber Essentials

Procreation is Cyber Essentials Certified and it is important to Procreation that controls to maintain the standard are implemented and reviewed. More information can be obtained from the CTO.

## 10. Malware Protection

The business uses software countermeasures and management procedures to protect itself against the threat of malicious software. All team members are expected to cooperate fully. All devices where possible must use anti malware protection. Users shall not install software or other active code that could impact Procreation or customer data without permission from the CTO. Users breaching this requirement may be subject to disciplinary action.

All obsolete, unused and unsupported software and utility software and programs shall be deleted. This control shall be refreshed regularly, but at least once a year in line with the Cyber Essentials certification.

## 11. Information security incidents and weaknesses

All breaches of this Policy, other policies and other information security incidents or suspected weaknesses are to be reported to the CTO. Information security events shall be 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.

## 12. 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 and that these plans are tested on a regular basis.

## 13. Electronic Commerce

B2B and other electronic commerce shall be secure and authenticated. Access to ecommerce data at rest shall be strictly controlled.

## 14. Reporting

The CTO shall keep the business informed of the information security status by means of regular reports and presentations.

## 15. Further Information

Further information and advice on this policy can be obtained from the CTO. Comments and suggestions to improve security are always welcome.

Signed by

CTO

Signature:

Agreed by

Name: ______________________________

I am fully aware of my personal responsibility regarding information security. I also agree that I have been provided with adequate security awareness training for me to do my job effectively whilst protecting Procreation’s information:

Signature: ______________________________ Date: ____________