PROCREATION UK LIMITED

CYBER ESSENTIALS POLICY
Version 1.3

1. Introduction & Purpose 2

2. Scope 2

3. Responsibilities 2

4. Legislation 2

5. Policy Framework 3

5.1. Team Contracts 3

5.2 Asset Management 3

5.3 Access to Systems 3

5.4 Cyber Essentials 4

6. Further Information 4

1. Introduction & Purpose

Data and information are vitally important to us. We all share a responsibility to make sure that it is kept safe and used appropriately. Without due care, it can be misplaced or leaked, which is serious enough without the added difficulty of having to protect it against increasingly proactive and sophisticated attempts at theft.

We have, therefore, adopted this policy to provide the necessary assurance that data and information held and processed by us is treated appropriately to keep it safe, and also to comply with data protection legislation.

This policy is a key component of our overall business management framework and provides the baseline for our information security efforts.The aim of this policy is to set out the rules governing the secure management of data and information by ensuring that all members of the team:

- are aware of and fully comply with the relevant legislation,
- create and maintain a level of awareness of the need for data and information security as an integral part of the day to day business,
- protect data and information that we receive and hold.

2. Scope

This policy applies to all data, information, software, applications (i.e. a service used but not downloaded), systems, networks (home, office and others), locations and users of our systems as well as hardware such as laptops, mobile devices, tablets, etc. used to access this, whether owned/ supplied by you, Procreation UK Limited or otherwise.

3. Responsibilities

Ultimate responsibility for data and information security rests with each team member. We cannot ensure that it is secure without you. You are all therefore individually responsible for managing and implementing this policy and related processes and procedures. This is particularly important as our team is so widespread and largely works autonomously.

All of you must, therefore, comply with our data and information security procedures, including the maintenance of data confidentiality, integrity and security. Failure to do so may result in our being unable to work with you and the termination of your contract.

You are also individually responsible for the security of your physical environment where data and information are processed and/or stored. Again this is particularly important as so many of us work outside the office. You are, together with Procreation UK Limited, responsible for the operational security of the information systems you use.

4. Legislation

Procreation UK Limited is obliged to abide by relevant legislation. It is also each team member's requirement – you may be held personally accountable for any breaches of data or information security for which you are responsible.

5. Policy Framework

5.1. Team Contracts

Your contract with Procreation UK Limited (together with this policy and others) sets out obligations regarding access to the organisation's systems, confidentiality and data security. Security requirements will also be addressed at the induction stage and updated from time to time.

On termination of your contract, all access rights will be removed and all associated accounts will be deleted or disabled, devices will be remote wiped (where possible) and any Procreation UK Limited assets must be returned immediately.

5.2 Asset Management

Devices include all computers, laptops, tablets and mobile phones that can access Procreation UK Limited data and information. It is each team member's responsibility to ensure that these devices meet the following criteria:

- keep devices safe and take care when using them in public spaces,
- devices and operating systems are supported by the supplier/manufacturer and get regular fixes (i.e. they are not obsolete),
- all obsolete/ unused/ unsupported software is deleted or disabled,
- anti-malware is installed (where available) and it updates and scans files and websites automatically,
- they must not be modified to remove restrictions imposed by a manufacturer or operator (i.e. 'phones should not be jailbroken),
- software/ applications are only installed from official providers,
- access requires a unique username and password/ passcode, and
- default passwords are changed for all devices (i.e. from the passwords that are automatically assigned when you first receive them) to a new strong password (at least 8 characters and not- guessable (e.g. not your child's birthday or dog's name) and changed regularly, particularly if you suspect your device or any software on them has been compromised in any way – don't forget voicemail.

5.3 Access to Systems

We will ensure that all software/applications used by the team are licensed in accordance with the provider's recommendations and such providers have appropriate terms in their contracts regarding data and information protection. Team members must use unique usernames and strong and unique passwords, which must be changed regularly, to access the software/applications. A respected password manager may be used for this.

When working outside the office you must ensure any router you connect to is protected by a firewall and password protected. Most home internet routers (BT, Virgin, Sky, etc.) have this built in by default – please check regularly.[1] and keep passwords private. Many others, e.g. coffee shops etc. may not be secure so please do not access Procreation UK Limited software or data via them unless there is a VPN in place.

Only team members who have a justified and approved business need shall be given access to certain systems, data and information. Administrator accounts:

- will be regularly reviewed to check the person has a business need for this access,
- must, where possible, have two-factor authentication for access to their accounts enabled,
- must have a strong password (i.e. at least eight characters, o one capitalised letter, o one number and o one special character (!@£$%&*)).

To check, open a web browser and type into the URL “192.168.0.1”. This will direct you to your home router login page. The username and password should be on the back of your router. Go to the settings and configurations and ensure “Firewall” is turned on/enabled.

5.4 Cyber Essentials

We use CyberSmart to obtain and maintain our annual Cyber Essentials certification. It is important that controls to maintain the standard are implemented and reviewed on a regular basis.

6. Further Information

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