iFormulate Ltd
Data Security Policy
Issue 1.0 19/12/2019

1. Introduction

This document sets out the measures to be taken by all employees of iFormulate Ltd (the "Company") and by the Company as a whole in order to protect data (electronic and otherwise) collected, held, and processed by the Company, and to protect the Company's computer systems, devices, infrastructure, computing environment, and any and all other relevant equipment (collectively, "IT Systems") from damage and threats whether internal, external, deliberate, or accidental.

For the purposes of this Policy, "data" shall refer to the following type(s) of data:

a) Minimal business-to-business contact information on individuals (email address, organisation, phone number(s) job title and address) and no personal data other than name. This information is held in a database and is principally used as the basis of a mailing list for the Company e-newsletter.

b) Electronic copies of emails sent and received by the Company are maintained in order to conduct regular business activities with clients, training course delegates, suppliers, business partners and other associates. These may also contain comparable contact information to that described above.;

c) Text documents, letters, contracts, presentations, scientific results and other general business documentation which is held in order to conduct regular business activities with clients, training course delegates, suppliers, business partners and other associates. This documentation is held principally on secure cloud data storage with some being held as hard copy in locked home-offices. Some of this documentation is commercially confidential to client companies, to iFormulate or to both.

For the purposes of this Policy, "personal data" shall carry the meaning defined in Article 4 of EU Regulation 2016/679 General Data Protection Regulation ("GDPR"): any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

2. Key Principles

2.1 All IT Systems and data are to be protected against unauthorised access.

2.2 All IT Systems and data are to be used only in compliance with relevant Company Policies.

2.3 All personal data must be used only in compliance with the GDPR and the Company's Data Protection Policy.

2.4 All employees of the Company and any and all third parties authorised to use the IT

Systems and data collected, held, and processed by the Company including, but not limited to, contractors and sub-contractors (collectively, "Users"), must ensure that they are familiar with this Policy and must adhere to and comply with it at all times.

2.5 The Directors of the Company (collectively "Directors") must ensure that all Users under their control and direction must adhere to and comply with this Policy at all times as required under paragraph 2.4.

2.6 All data must be managed securely in compliance with all relevant parts of the GDPR and all other laws governing data protection whether now or in the future in force.

2.7 All data must be classified appropriately (including, but not limited to, personal data, sensitive personal data, and confidential information). All data so classified must be handled appropriately in accordance with its classification.

2.8 All data, whether stored on IT Systems or in hardcopy format, shall be:

2.8.1 available only to those Users with a legitimate need for access.

2.8.2 protected against unauthorised access and/or processing.

2.8.3 protected against loss and/or corruption.

2.9 All IT Systems are to be installed, maintained, serviced, repaired, and upgraded by the Directors or by such third party/parties as the Directors may from time to time authorise.

2.10 The responsibility for the security and integrity of all IT Systems and the data stored thereon (including, but not limited to, the security, integrity, and confidentiality of that data) lies with the Directors unless expressly stated otherwise.

2.11 The responsibility for the security and integrity of data that is not stored on the IT Systems lies with the Directors.

2.12 All breaches of security pertaining to the IT Systems or any data stored thereon (including personal data) shall be reported and subsequently investigated by the Directors.

2.13 All breaches of security pertaining to data that is not stored on the IT Systems (including personal data) shall be reported and subsequently investigated by the Directors.

2.14 All Users must report any and all security concerns relating to:

2.14.1 the IT Systems or to the data (including personal data) stored thereon immediately to the Directors.

2.14.2 data that is not stored on the IT Systems (including personal data) immediately to the Directors.

3. Department Responsibilities

3.1 The Directors shall be responsible for the following:

a) ensuring that all IT Systems are assessed and deemed suitable for compliance with the Company's security requirements;

b) ensuring that IT security standards within the Company are effectively implemented and regularly reviewed as well as recording and acting on the outcome of such reviews;

c) ensuring that all Users are kept aware of the IT-related requirements of this Policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force including, but not limited to, the GDPR and the Computer Misuse Act 1990.

d) ensuring that all other data processing systems and methods are assessed and deemed suitable for compliance with the Company's security requirements;

e) ensuring that data security standards within the Company are effectively implemented and regularly reviewed, as well as recording and acting on the outcome of such reviews;

f) ensuring that all Users are kept aware of the non-IT-related requirements of this Policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force including, but not limited to, the GDPR.

g) assisting all Users in understanding and complying with the IT-related aspects of this Policy;

h) providing all Users with appropriate support and training in IT security matters and use of IT Systems;

i) ensuring that all Users are granted levels of access to IT Systems and data that are appropriate for each User, taking into account their job role, responsibilities, and any special security requirements;

j) receiving and handling all reports relating to IT security matters and taking appropriate action in response including any reports relating to personal data;

k) taking proactive action, where possible, to establish and implement IT security procedures and raise User awareness;

l) ensuring that all data stored within the IT Systems is archived and securely stored.

m) assisting all Users in understanding and complying with the non-IT-related aspects of this Policy;

n) receiving and handling reports concerning non-IT-related data security matters and taking appropriate action in response including any reports relating to personal data;

4. Users' Responsibilities

4.1 All Users must comply with all relevant parts of this Policy at all times when using the IT Systems and data.

4.2 All Users must use the IT Systems and data only within the bounds of UK law and must not use the IT Systems or data for any purpose or activity which is likely to contravene any UK law whether now or in the future in force.

4.3 Users must immediately inform the Directors of any and all security concerns relating to the IT Systems or data.

4.4 Users must immediately inform the Directors of any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems.

4.5 Any and all deliberate or negligent breaches of this Policy by Users will be handled as appropriate under the Company's disciplinary procedures.

5. Software Security Measures

5.1 All software in use on the IT Systems (including, but not limited to, operating systems, individual software applications, and firmware) will be kept up-to-date and any and all relevant software updates, patches, fixes, and other intermediate releases will be applied at the sole discretion of the Directors. This provision does not extend to upgrading software to new 'major releases' (e.g. from version 1.0 to version 2.0), only to updates within a particular major release (e.g. from version 1.0 to version 1.0.1 etc.). Unless a software update is available free of charge it will be classed as a major release, falling within the remit of new software procurement and outside the scope of this provision.

5.2 Where any security flaw is identified in any software that flaw will be either fixed immediately or the software may be withdrawn from the IT Systems until such time as the security flaw can be effectively remedied. If the security flaw affects, is likely to affect, or is suspected to affect any personal data, the Directors shall act to resolve the issue immediately.

5.3 No Users may install any software of their own, whether that software is supplied on physical media or whether it is downloaded, without the approval of the Directors. Any software belonging to Users must be approved by the Directors and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject.

6. Anti-Virus Security Measures

6.1 IT Systems (including all computers and servers) will be protected with suitable anti-virus, firewall, and other suitable internet security software. All such software will be kept up-to-date with the latest software updates and definitions.

6.2 All IT Systems protected by anti-virus software will be subject to a full system scan at regular intervals.

6.3 All physical media (e.g. USB memory sticks or disks of any kind) used by Users for transferring files must be virus-scanned before any files may be transferred. Such virus scans shall be performed upon connection / insertion of mediaby the User.

6.4 Users shall be permitted to transfer files using cloud storage systems only with the approval of the Directors. All files downloaded from any cloud storage system must be scanned for viruses during the download process.

6.5 Any files being sent to third parties outside the Company, whether by email, on physical media, or by other means (e.g. shared cloud storage) must be scanned for viruses before being sent or as part of the sending process, as appropriate. All email attachments are scanned automatically upon sending.

6.6 Where any virus is detected by a User this must be reported immediately to the Directors (apply even where the anti-virus software automatically fixes the problem). The Directors shall promptly take any and all necessary action to remedy the problem. In limited circumstances this may involve the temporary removal of the affected computer or device. Wherever possible a suitable replacement computer or

device will be made available to limit disruption to the User.

6.7 If any virus or other malware affects, is likely to affect, or is suspected to affect any personal data, in addition to the above, the issue must be reported immediately to the Directors.

6.8 Where any User deliberately introduces any malicious software or virus to the IT Systems this will constitute a criminal offence under the Computer Misuse Act 1990 and will be handled as appropriate under the Company's disciplinary procedures.

7. Hardware Security Measures

7.1 Wherever practical, IT Systems will be located in rooms which may be securely locked when not in use or, in appropriate cases, at all times whether in use or not (with authorised Users being granted access by means of a key, smart card, door code or similar). Where access to such locations is restricted, Users must not allow any unauthorised access to such locations for any reason.

7.2 All mobile devices (including, but not limited to, laptops, tablets, and smartphones) provided by the Company should always be transported securely and handled with care. In circumstances where such mobile devices are to be left unattended they should be placed inside a lockable case or other suitable container. Users should make all reasonable efforts to avoid such mobile devices from being left unattended at any location other than their private homes or Company premises. If any such mobile device is to be left in a vehicle it must be stored out of sight and, where possible, in a locked compartment.

8. Organisational Security

8.1 All Users handling data (and in particular, personal data) shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to such data, whether in the workplace or otherwise.

8.2 Methods of collecting, holding, and processing data (and in particular, personal data) shall be regularly evaluated and reviewed.

8.3 All personal and non-personal data held by the Company shall be reviewed periodically, by the Directors.

8.4 All Users handling personal data will be bound to do so in accordance with the principles of the GDPR and the applicable Company Policies by contract.

8.5 No data, personal or otherwise, may be shared informally and if a User requires access to any data, personal or otherwise, that they do not already have access to, such access should be formally requested the Directors.

8.6 No data, personal or otherwise, may be transferred to any unauthorised User without the authorisation of the Directors.

8.7 All data must be handled with care at all times and should not be left unattended or on view to unauthorised Users or other parties at any time.

9. Access Security

9.1 Access to all IT Systems and data shall be determined by the Directors. Users shall not be granted access to any IT Systems or data which are not reasonably required for

the fulfilment of their job roles.

9.2 All IT Systems (and in particular mobile devices including, but not limited to, laptops, tablets, and smartphones) shall be protected with a secure password or passcode, or such other form of secure log-in system as the Directors may deem appropriate.

9.3 Passwords should be kept secret by each User. Under no circumstances should a User share their password with anyone else. If a User has reason to believe that another individual has obtained their password, they should change their password immediately and report the suspected breach of security to the Directors.

9.4 If a User forgets their password, this should be reported to the Directors who will restore the User's access to the IT Systems.

9.5 Users should not write down passwords and under no circumstances should passwords be left on display for others to see (e.g. by attaching a note to a computer display).

9.6 All IT Systems with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) shall be protected, where possible, with a password protected screensaver that will activate after a period of inactivity.

9.7 All mobile devices (including, but not limited to, laptops, tablets, and smartphones) provided by the Company shall be set to lock, sleep, or similar, after a period of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake, or similar.

9.8 Users may not use any software which may allow outside parties to access the IT Systems without the express consent of the Directors.

9.9 Users may connect their own devices (including, but not limited to, laptops, tablets, and smartphones) to the IT Systems subject to the approval of the Directors.. Users' use of their own devices shall be subject to, and governed by, all relevant Company Policies (including, but not limited to, this Policy) while those devices are connected to the Company network or to any other part of the IT Systems. The Directors shall reserve the right to request the immediate disconnection of any such devices without notice.

10. Data Storage Security

10.1 All data stored in electronic form, and in particular personal data, should be stored securely using passwords and, where feasible, data encryption.

10.2 All data stored in hardcopy format or electronically on removable physical media, and in particular personal data, should be stored securely in a locked location.

10.3 No data, and in particular personal data, should be transferred to any computer or device personally belonging to a User unless the User in question is a contractor or sub-contractor working on behalf of the Company and that User has agreed to comply fully with the Company's Data Protection Policy and the GDPR.

11. Data Protection

11.1 All personal data (as defined in the GDPR) collected, held, and processed by the Company will be collected, held, and processed strictly in accordance with the principles of the GDPR, the provisions of the GDPR and the Company's Data

Protection Policy (which is published on the Company's website).

11.2 All Users handling data for and on behalf of the Company shall be subject to, and must comply with, the provisions of the Company's Data Protection Policy at all times. In particular, the following shall apply:

a) All emails containing personal data and/or other data covered by this Policy must be marked "confidential";

b) Personal data and/or other data covered by this Policy may be transmitted over secure networks only; transmission over unsecured networks is not permitted under any circumstances;

c) All personal data and/or other data covered by this Policy to be transferred physically, including that on removable electronic media, shall be transferred in a suitable container marked "confidential".

d) Where any personal data and/or other data covered by this Policy is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the User must lock the computer and screen before leaving it.

11.3 Any questions relating to data protection should be referred to the Directors.

12. **Deletion and Disposal of Data**

12.1 When any data, and in particular personal data, is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it must be securely deleted.

13. **Reporting Security Breaches**

13.1 All concerns, questions, suspected breaches, or known breaches that relate to the IT Systems, to other data covered by this Policy or that involve personal data shall be referred immediately to the Directors who shall handle the matter in accordance with the Company's Data Protection Policy.

13.2 Upon receiving a question or notification of a breach, the Directors shall, within as short a time as is reasonable, assess the issue including, but not limited to, the level of risk associated therewith, and shall take any and all such steps deemed necessary to respond to the issue.

13.3 Under no circumstances should a User attempt to resolve a security breach on their own without first consulting the Directors. Users may only attempt to resolve security breaches with the express permission of the Directors.

13.4 All security breaches, howsoever remedied, shall be fully documented.

14. **Policy Review**

The Company shall review this Policy not less than annually and otherwise as required in order to ensure that it remains up-to-date and fit for purpose. All questions, concerns, and other feedback relating to this Policy should be communicated to the Directors.

15. Implementation of Policy

This Policy shall be deemed effective as of 18th July 2019. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name:	James Bullock
Position:	Director
Date:	19/12/2019
Due for Review by:	19/12/2020
Signature:	

Name:	David Calvert
Position:	Director
Date:	19/12/2019
Due for Review by:	19/12/2020
Signature:	