Information Security Policy

1 Introduction

1.1 The Company is committed to the highest standards of information security and treats confidentiality and data security extremely seriously.

1.2 This purpose of this policy is to:

1.2.1 protect against potential breaches of confidentiality;

1.2.2 ensure all our information assets and IT facilities are protected against damage, loss or misuse;

1.2.3 support our Data Protection Policy in ensuring all staff are aware of and comply with UK law and our own procedures applying to the processing of data; and

1.2.4 increase awareness and understanding in the Company of the requirements of information security and the responsibility of staff to protect the confidentiality and integrity of the information that they themselves handle.

1.3 The Company's data protection officer, Danielle Coletti, is responsible for the monitoring and implementation of this policy. If you have any questions about the content of this policy or other comments you should contact the data protection officer.

2 Scope

2.1 The information covered by the policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the Company, in whatever media. This includes information held on computer systems, hand-held devices, phones, paper records, and information transmitted orally.

2.2 This policy applies to all staff, which for these purposes includes employees, temporary and agency workers, other contractors, interns and volunteers.

2.3 All staff must be familiar with this policy and comply with its terms.

2.4 This policy does not form part of any employee's contract of employment and the Company may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

3 General principles

3.1 All Company information must be treated as commercially valuable and be protected from loss, theft, misuse or inappropriate access or disclosure.

3.2 Staff should discuss with line managers the appropriate security arrangements which are appropriate and in place for the type of information they access in the course of their work.

3.3 Staff should ensure they attend any information security training they are invited to unless otherwise agreed by line managers.

3.4 Information is owned by the Company and not by any individual or team.

3.5 Company information must only be used in connection with work being carried out for the Company and not for other commercial or personal purposes.

4 Information management

4.1 Information gathered should not be excessive and should be adequate relevant, accurate and up to date for the purposes for which it is to be used by the Company.

4.2 Information will be kept for no longer than is necessary. All confidential material that requires disposal must be shredded or, in the case of electronic material, securely destroyed, as soon as the need for its retention has passed.

5 Human resources information

5.1 Given the internal confidentiality of personnel files, access to such information is limited to those members of the Company who need access to it for operational reasons in compliance with our Data Protection Policy. Except as provided in individual roles, other staff are not authorised to access that information.

5.2 Any staff member in a management or supervisory role must keep personnel information confidential.

5.3 Staff may ask to see their personnel files in accordance with the relevant provisions of the Data Protection Act 2018.

6 Access to offices and information

6.1 Office doors must be kept secure at all times and visitors must not be given keys or access codes.

6.2 Documents containing confidential information and equipment displaying confidential information should be positioned in a way to avoid them being viewed by people passing by, e.g. through office windows.

6.3 Visitors should be required to sign in at reception, accompanied at all times and never be left alone in areas where they could have access to confidential information.

6.4 Wherever possible, visitors should be seen in meeting rooms. If it is necessary for a member of staff to meet with visitors in an office or other room which contains Company information, then steps should be taken to ensure that no confidential information is visible.

6.5 At the end of each day, or when desks are unoccupied, all paper documents, backup systems and devices containing confidential information must be securely locked away.

7 Computers and IT

7.1 Use password protection and encryption where available on Company systems to maintain confidentiality.

7.2 Computers and other electronic devices must be password protected. Passwords should not be written down or given to others.

7.3 Computers and other electronic devices should be locked when not in use to minimise the risk of accidental loss or disclosure.

7.4 Confidential information must not be copied onto floppy disk, removable hard drive, CD or DVD or memory stick/ thumb drive without the express permission of a director or the data protection officer. Data copied onto any of these devices should be deleted as soon as possible and stored on the Company's computer network in order for it to be backed up.

7.5 All electronic data must be securely backed up in accordance with company policy.

7.6 Staff should ensure they do not introduce viruses or malicious code on to Company systems. Software should not be installed or downloaded from the internet without it first being virus checked.

8 Communications and transfer

8.1 Staff should be careful about maintaining confidentiality when speaking in public places.

8.2 Confidential information should be marked 'confidential' and circulated only to those who need to know the information in the course of their work for the Company.

8.3 Confidential information must not be removed from the Company's offices except where that removal is temporary and necessary.

8.4 In the limited circumstances when confidential information is permitted to be removed from the Company's offices, all reasonable steps must be taken to ensure that the integrity of the information and confidentiality are maintained. Staff must ensure that confidential information is:

8.4.1 not transported in see-through or other un-secured bags or cases;

8.4.2 not read in public places (e.g. waiting rooms, cafes, trains); and

8.4.3 not left unattended or in any place where it is at risk (e.g. in conference rooms, car boots, cafes).

8.5 Postal, document exchange (DX), fax and email addresses and numbers should be checked and verified before information is sent to them. Particular care should be

taken with email addresses where auto-complete features may have inserted incorrect addresses.

8.6 All sensitive or particularly confidential information should be encrypted before being sent by email, or be sent by tracked DX or recorded delivery.

8.7 Sensitive or particularly confidential information should not be sent by fax unless you can be sure that it will not be inappropriately intercepted at the recipient fax machine.

9 Home working

9.1 Staff should not take confidential or other information home without authority and only do so where appropriate technical and practical measures are in place within the home to maintain the continued security and confidentiality of that information.

9.2 In the limited circumstances in which staff are permitted to take Company information home, staff must ensure that:

9.2.1 confidential information must be kept in a secure and locked environment where it cannot be accessed by family members or visitors; and

9.2.2 all confidential material that requires disposal must be shredded or, in the case of electronic material, securely destroyed, as soon as any need for its retention has passed.

9.3 Staff should not store confidential information on home computers (PCs, laptops or tablets).

10 Transfer to third parties

10.1 Third parties should only be used to process Company information in circumstances where written agreements are in place ensuring that those service providers offer appropriate confidentiality, information security and data protection undertakings.

10.2 Staff involved in setting up new arrangements with third parties or altering existing arrangements should consult the data protection officer or a director for guidance and authority.

11 Overseas transfer

11.1 There are restrictions on international transfers of personal data. Staff must not transfer personal data internationally at all without first consulting the data protection officer or a director.

12 Reporting breaches

12.1 All staff have an obligation to report actual or potential data protection compliance failures to the data protection officer, a director or appropriate manager. This allows the Company to:

12.1.1 investigate the failure and take remedial steps if necessary; and

12.1.2 make any applicable notifications.

13 Consequences of failing to comply

13.1 The Company takes compliance with this policy very seriously. Failure to comply puts both staff and the Company at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action, which may result in dismissal.

13.2 Staff with any questions or concerns about anything in this policy should not hesitate to contact the data protection officer.

I have read and understood this policy and agree to abide by its terms.

Signed .....

Name .....

Date .....