THE BIODIVERSITY CONSULTANCY

THE BIODIVERSITY CONSULTANCY LIMITED

DATA PROTECTION POLICY

April 2018

1. INTRODUCTION

1.1 The Company holds personal data about job applicants, employees, clients, suppliers and other individuals for a variety of business purposes.

1.2 This policy sets out how the Company seeks to protect personal data and ensure staff understand the rules governing their use of personal data to which they have access in the course of their work.

1.3 In particular, this policy requires staff to ensure that the Managing Director should be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

1.4 The Managing Director 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 Manager and HR & Communications Manager.

2. SCOPE

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

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

2.3 This policy supplements the Company's other policies.

2.4 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. DEFINITIONS

In this policy:

"business purposes" means the purposes for which personal data may be used by the Company, eg personnel, administrative, financial, regulatory, payroll and business development purposes and health and safety;

"personal data" means information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts. This includes expression of opinion about the individual and any indication of someone else's intentions towards the individual;

"sensitive personal data" means personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, sexual life, criminal offences, or related proceedings. Any use of sensitive personal data must be strictly controlled in accordance with this policy;

"processing data" means obtaining, recording, holding or doing anything with data, such as organising, using, altering, retrieving, disclosing or deleting it.

4. GENERAL PRINCIPLES

4.1 The Company's policy is to process personal data in accordance with the applicable data protection laws and rights of individuals as set out below. All employees have personal responsibility for the practical application of the Company's data protection policy.

4.2 The Company will observe the following principles in respect of the processing of personal data:

(a) to process personal data fairly and lawfully in line with individuals' rights;

(b) to make sure that any personal data processed for a specific purpose are adequate, relevant and not excessive for that purpose;

(c) to keep personal data accurate and up to date;

(d) to keep personal data for no longer than is necessary;

(e) to keep personal data secure against loss or misuse;

(f) not to transfer personal data outside the EEA (which includes the EU countries, Norway, Iceland and Liechtenstein) without adequate protection.

5. FAIR AND LAWFUL PROCESSING

5.1 Staff should generally not process personal data unless:

(a) the individual whose details are being processed has consented to this;

(b) the processing is necessary to perform the Company's legal obligations or exercise legal rights, or

(c) the processing is otherwise in the Company's legitimate interests and does not unduly prejudice the individual's privacy.

5.2 When gathering personal data or establishing new data protection activities, staff should ensure that individuals whose data is being processed receive appropriate data protection notices to inform them how the data will be used. There are limited exceptions to this notice requirement. In any case of uncertainty as to whether a notification should be given, staff should contact the HR & Communications Manager & Data Protection Manager.

5.3 It will normally be necessary to have an individual's explicit consent to process 'sensitive personal data', unless exceptional circumstances apply or the processing is

necessary to comply with a legal requirement. The consent should be informed, which means it needs to identify the relevant data, why it is being processed and to whom it will be disclosed. Staff should contact the Data Protection Manager & HR & Communications Manager for more information on obtaining consent to process sensitive personal data.

6. ACCURACY, ADEQUACY, RELEVANCE AND PROPORTIONALITY

6.1 Staff should make sure data processed by them is accurate, adequate, relevant and proportionate for the purpose for which it was obtained. Personal data obtained for one purpose should generally not be used for unconnected purposes unless the individual has agreed to this or would otherwise reasonably expect the data to be used in this way.

6.2 Individuals may ask the Company to correct personal data relating to them which they consider to be inaccurate. If a member of staff receives such a request and does not agree that the personal data held is inaccurate, they should nevertheless record the fact that it is disputed and inform the HR & Communications Manager and Data Protection Manager.

6.3 Staff must ensure that personal data held by the Company relating to them is accurate and updated as required. If personal details or circumstances change, staff should inform the Data Protection Manager so the Company's records can be updated.

7. SECURITY

Staff must keep personal data secure against loss or misuse. Personal data must not be provided to third parties unless it is necessary to do so and in accordance with the data protection principles. Where the Company uses external organisations to process personal data on its behalf additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal data. Staff should consult the HR & Communications Manager to discuss the necessary steps to ensure compliance when setting up any new agreement or altering any existing agreement.

8. DATA PROCESSORS

Where any personal data that we hold is passed to third parties to process on our behalf this must only be done where we have satisfied ourselves as to the suitability of such third party and have a formal written agreement in place. All such agreements must be approved by the Data Protection Manager and HR & Communications Manager.

9. DATA RETENTION

Personal data should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances including the reasons why the personal data were obtained.

10. INTERNATIONAL TRANSFER

Staff should not transfer personal data internationally without first consulting the Data Protection Manager and HR & Communications Manager. There are restrictions on international transfers of personal data from the UK to other countries because of the need to ensure adequate safeguards are in place to protect the personal data. Staff unsure of what arrangements have been or need to be put in place to address this requirement should contact the Data Protection Manager and HR & Communications Manager.

Rights of individuals

10.1 Individuals are entitled (subject to certain exceptions) to request access to information held about them. All such requests should be referred immediately to the Data Protection Manager. This is particularly important because the Company must respond to a valid request within the legally prescribed time limits.

10.2 Any member of staff who would like to correct or request information that the Company holds relating to them should contact the Data Protection Manager. It should be noted that there are certain restrictions on the information to which individuals are entitled under applicable law.

10.3 Staff should not send direct marketing material to someone electronically (eg by email) unless they have consented to receiving such communications. Staff should abide by any request from an individual not to use their personal data for direct marketing purposes and should notify the Data Protection Manager about any such request. Staff should contact the HR & Communications Manager for advice on direct marketing before starting any new direct marketing activity.

11. REPORTING BREACHES

Staff have an obligation to immediately report actual or potential data protection compliance failures to the Managing Director, HR & Communications Manager and Data Protection Manager as soon as they are identified. This allows the Company to:

(a) investigate the failure and take remedial steps if necessary; and

(b) make any applicable reports to the Information Commissioner and others. We have a very short period of time to make such reports.

12. CONSEQUENCES OF FAILING TO COMPLY

12.1 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.

12.2 Staff with any questions or concerns about anything in this policy should not hesitate to discuss these with the Data Protection Manager.

HR & Communications Manager: Katherin Pertsinidis, katherin@thebiodiversityconsultancy.com

Data Protection Manager: Amelia Topham, amelia.topham@thebiodiversityconsultancy.com

Managing Director: David Tassell, david.tassell@thebiodiversityconsultancy.com