DATA PROTECTION AND INFORMATION SECURITY POLICY STATEMENT

DATA PROTECTION AND INFORMATION SECURITY POLICY STATEMENT

CONTENTS

01 INTRODUCTION

The General Data Protection Regulations (GDPR) came into force on 25 May 2018, replacing the EU Data Protection Directive and superseding the Data Protection Act 1998. It was transposed into UK law through the Data Protection Act 2018. The purpose of the GDPR is to protect the rights and freedoms of individuals and ensure that personal data is not processed without their knowledge, and wherever possible, that it is processed with their consent.

Urban Initiatives Studio (UIS) needs to collect and use certain types of information about people with whom it deals. These people include current, past and prospective employees, suppliers, customers and others with whom it communicates. In addition, UIS may occasionally be required by law to collect and use certain types of information of this kind to comply with the requirements of government departments for business data, for example. This personal information must be dealt with properly and in accordance with the Data Protection Act 2018.

This policy sets out how Urban Initiatives Studio will handle the personal data it handles in the course of its business, and will comply with the Data Protection principles set out in GDPR.

02 DATA PROTECTION PRINCIPLES

Urban Initiatives Studio is committed to processing data in accordance with its responsibilities under data protection legislation.

Article 5 of the GDPR requires that personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

03 APPLICATION OF THE GDPR PRINCIPLES

Urban Initiatives Studio will, through appropriate management, strict application of criteria and controls:

- Observe fully the rules regarding the fair collection and use of information;
- Meet its legal obligations to specify the purposes for which information is used;
- Collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality and accuracy of information used;
- Apply strict checks to determine the length of time information is held;
- Ensure that the rights of people about whom information is held, are able to be fully exercised under the Act. (These include: the right to be informed that processing is being undertaken, the right of access to one's personal information, the right to prevent processing in certain circumstances and the right to correct rectify, block or erase information which is regarded as wrong information);
- Take appropriate technical and organisational security measures to safeguard personal information; and
- Ensure that personal information is not transferred abroad without suitable safeguards or consents.

04 DATA SECURITY

The Sixth principle of the data protection principles requires date to be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

UIS shall ensure that all of its security measures are sufficiently robust and state of the art and that they are appropriate to protect the risks of the processing activity. Those risks will vary in relation to the different types of data being processed.

Security measures shall be reviewed periodically to ensure they remain effective and commensurate with the risks of processing.

The greatest risk to data security comes not from technological factors, but from human error. All staff will receive training appropriate to their role in handling data on the requirements of data protection legislation, the importance of data security, and the risks involved in their own data processing.

Particular care must be taken if staff members are taking personal data outside of UIS's premises. Personal data shall not be taken out of the UIS office without informing a Director.

Portable equipment (including but not limited to laptop computers and removable media such as USB drives and SD cards) shall not be used to store personal data for which UIS is responsible.

Where work is undertaken on laptops, personal data shall only be accessed via a remote, password-protected log-in to UIS servers.

05 ADDITIONAL ISSUES

5.1 GENERAL RESPONSIBILITY

Urban Initiatives Studio directors have specific responsibility for data protection.

5.2 RESPONSIBILITY OF DATA HANDLERS

Everyone managing and handling personal information is responsible for following good data protection practice as set out in this policy.

5.3 TRAINING

Everyone managing and handling personal information should have appropriate training to do so. This training consists of:

a) the training material within staff handbooks

b) additional material available from UIS directors

c) external courses

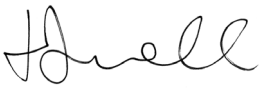
5.4 SUPERVISION

Everyone managing and handling personal information will be appropriately supervised so that:

- anybody wanting to make enquiries about handling personal information knows what to do;
- queries about handling personal information are promptly and courteously dealt with;
- methods of handling personal information are clearly described;
- a regular review and audit is made of the way personal data is managed;
- methods of handling personal information are regularly assessed and evaluated; and
- performance with handling personal information is regularly assessed and evaluated.

5.5 RIGHTS OF STAFF

Members of staff have the rights of a 'Data Subject' briefly described in section 3 above. A member of staff is entitled to find out what information is held about him/her, and have any errors corrected. Staff should route requests for information or for correction of data to the Director of Human Resources.



Signed:.....

Hugo Nowell

Designation: Director

Date of issue: 22 May 2018

.....