Usel Data Protection Policy

Name	Usel Data Protection Policy
Reference	Corporate Services
Version	V1
Date Created	05/05/17
Last Reviewed	

Introduction

1. Usel is fully committed to complying with the Data Protection Act 1998 which came into force on 1 March 2000.

2. We will follow procedures to ensure that all employees, contractors, agents, consultants and other parties who have access to any personal information held by or on behalf of us are fully aware of and abide by their duties and responsibilities under the Act

Statement of Policy

3. We need to collect and use information about people with whom we work in order to carry out our business and provide our services. These may include Board Members, members of the public, current, past and prospective employees, clients, customers and suppliers. In addition, we may be required by law to collect and use information. All personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it is on paper, in computer records or recorded by any other means.

Data Protection Principles

4. We fully support and comply with the eight principles of the Act. In summary, this means personal information must be:

1. Processed fairly and lawfully;
2. Processed for limited purposes and in an appropriate way;
3. Relevant and sufficient for the purpose;
4. Accurate;
5. Kept for as long as is necessary and no longer;
6. Processed in line with individuals' rights;
7. Secure
8. Only transferred to other countries that have suitable data protection controls.

Registration with the Information Commissioner's Office (ICO)

5. Our purpose for holding personal information and a general description of the categories of people and organisations to which we may disclose it are listed in the Information Commissioner's Data Protection Register.

https://ico.org.uk/ESDWebPages/Entry/Z6155742

Usel ensures its entry in the ICO register is reviewed annually to ensure it remains accurate and appropriate at all times.

• Our Head of Corporate Services will review the current registration on an annual basis and highlight any required changes or amendments to the register, including adding an additional purpose to the notification or altering or removing a notification entry, to the immediate attention to the Information Standards Officer.

Disclosure of Personal Information

6. Strict conditions apply to the passing of personal information both internally and externally. We will not disclose personal information to any third party unless we believe it is lawful to do so. Respect to confidentiality will be given, where appropriate. In certain circumstances, information relating to staff acting in a business capacity may be made available provided:

- we have the statutory power or are required by law to do so; or
- the information is clearly not intrusive in nature; or
- the member of staff has consented to the disclosure; or
- the information is in a form that does not identify individual employees.

Handling of Personal Information

7. All staff with access to data will, through appropriate training and responsible management:

i. Fully observe conditions regarding the fair collection and use of personal information;
ii. Meet our legal obligations to specify the purposes for which personal information is used;
iii. Collect and process appropriate personal information only to the extent that it is needed to fulfill operational needs or to comply with any legal requirements;
iv. Ensure the quality of personal information used;
v. Apply strict checks to determine the length of time personal information is held;
vi. Ensure that the rights of people about whom information is held can be fully exercised under the Act;
vii. Take appropriate technical and organisational security measures to safeguard personal information;
viii. Ensure personal data is secured to prevent access by unauthorised individuals and that all information is kept in adequate storage in line with the information assurance policy;
ix. Ensure personal information is not transferred abroad without adequate safeguards.

Compliance

8. We will ensure that:

i. There is someone with specific responsibility for data protection in the organisation;
ii. All staff receive annual awareness of the Data Protection Act;
iii. Everyone managing and handling personal information understands that they are directly and personally responsible for following good data protection practice;
iv. Only staff who need access to personal information as part of their duties are authorised to do so;
v. Everyone managing and handling personal information is appropriately trained to do so;
vi. Everyone managing and handling personal information is appropriately supervised;
vii. Anyone wanting to make enquiries about handling personal information knows what to do;
viii. Queries about handling personal information are promptly and courteously dealt with;
ix. Methods of handling personal information are clearly described;
x. An audit of personal information is conducted on an annual basis. This will include an assessment and evaluation to ensure that all personal information held is accurate and up to date and that adequate controls are in place to ensure information is managed and stored appropriately.

9. To assist in achieving compliance, we have:

i. Appointed the Head of Corporate Services as the officer with overall responsibility for data protection within the organisation;
ii. Provided all staff with access to data protection online training that will be refreshed on an annual basis and data protection guidance;
iii. Appointed a Compliance Officer to ensure staff compliance with the data protection principles and adherence to the business area procedures;
iv. Monitoring procedures in place to ensure business area adherence with the Information Assurance Policy (annually);
v. Registered Uesl's purpose for holding personal information with the Information Commissioner, and provided a general description of the categories of people and organisations to which we may disclose it; and
vi. Implemented a procedure to ensure that personal data remains complete, accurate and up to date. This information will be reviewed on an annual basis.

Staff Responsibilities

10. All staff have a responsibility to protect the personal information held by Usel. They will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

i. They participate in training regarding the handling of personal information;
ii. Paper files and other records or documents containing personal / sensitive data are kept in a secure environment;
iii. Personal data held on computers and computer systems is protected by the use of secure passwords which, where possible, have forced changes periodically;
iv. Individual passwords are not easily compromised;
v. All personal data which staff provide to Usel is accurate and up to date and Usel is informed of any errors, corrections or changes.

11. If and when, as part of their responsibilities, staff collect information about other people, they must comply with the policy and business area procedures. No one should disclose personal information outside this guidance or use personal data held on others for their own purposes.

Third Party Users of Personal Information

12. Any third parties who are users of personal information supplied by Usel will be required to confirm and demonstrate that they will abide by the requirements of the Act.

Policy Awareness

13. A copy of this policy statement will be given to all new members of staff and relevant third parties. Existing staff and any relevant third parties will be advised of the policy which will be posted on our intranet site (Usel Connect) and issued in staff handbooks, as will any subsequent revisions. All staff and relevant third parties are to be familiar with and comply with this policy at all times.