Data Protection Policy

CSW Group's data protection policy sets out the company's commitment to protecting personal data and how it implements that commitment with regards to the collection and use of it. It also sets out how it complies with the principles and compliance with all relevant UK and EU laws in respect of personal data, and to protecting the "rights and freedoms" of individuals whose information CSW collects in accordance with the General Data Protection Regulation (GDPR). To support this, CSW has developed, implemented and continuously improves an information management system (IMS).

Data Protection Principles

Personal data must be processed in accordance with six 'Data Protection Principles.' It must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

Background to the General Data Protection Regulation ('GDPR')

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of living individuals, and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.
More information on GDPR can be found directly from: www.ico.gov.uk

We are accountable for these principles and must be compliant and implement their requirements.

1. CSW Data Protection Policy Statement

As a registered data processor, CSW is committed to complying with data protection legislation and good practice including:

a. processing personal information only in order to meet our legitimate operational needs whilst fulfilling legal requirements

b. collecting only the minimum personal information required for these purposes and not processing excessive personal information;

c. supporting the data controller in their role in providing clear information to individuals about how their personal information will be used and by whom;

d. only processing relevant and adequate personal information;

e. processing personal information fairly and lawfully;

f. maintaining an inventory of the categories of personal information processed by CSW Group and establishing appropriate retention periods for this;

g. keeping personal information accurate and, where necessary, up to date;

h. retaining personal information only for as long as is necessary for legal or regulatory reasons or, for legitimate organisational purposes;

i. respecting individuals' rights in relation to their personal information, including their right of subject access and overall ensuring that data subjects' rights can be appropriately exercised

j. keeping all personal information secure;

k. only transferring personal information outside the EU in circumstances where it can be adequately protected;

l. developing, implementing and continually improving a IMS to enable this policy to be implemented;

m. providing data protection training for all staff and promoting good practice in data protection;

n. ensuring that staff handling personal data know where to find further guidance;

o. ensuring that queries about data protection, internal and external to the organisation, are dealt with effectively and promptly;

p. where appropriate, identifying internal and external stakeholders and the degree to which they are involved in the IMS; and ensuring that data processing/sharing agreements are applied to them and when processing/sharing data to them and other third parties;

q. the identification of workers with specific responsibility and accountability for the IMS;

r. ensuring that a nominated officer is responsible for data protection compliance and is the point of contact for all data protection issues;

s. that complaints and/or breaches of data security are dealt with in accordance with Information Commissioners Office (ICO) procedures.

2. Policy Statement application

The policy applies to all employees, volunteers and outsourced suppliers of CSW. Any breach of the GDPR or this IMS will be dealt with under CSW's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

Partners and any third parties working with or for CSW, and who have or may have access to personal information, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by CSW without having first entered into a data

confidentiality agreement which imposes on them obligations no less onerous than those to which CSW is committed, and which gives CSW the right to audit compliance with the agreement.

3. Responsibilities

Chief Executive has overall responsibility for compliance with the GDPR.

The Director of Information and Innovation acts, on behalf of the Chief Executive, as the company's **Data Protection Officer**. He is responsible for maintaining the organisation's registration with the Data Protection Registrar and for oversight of all issues relating to GDPR and Data Protection.

All staff (including permanent, fixed term, casual temporary, agency staff and volunteers) are required to:

- adhere to the Data Protection and GDPR principles in their handling and recording of personal information, whether on computer or paper
- complete data protection training in line with company Essential Training Procedures and any additional company requirements
- comply with CSW's Data Protection and Information Security Procedures
- keep personal data securely and in line with the Information Management Security procedures
- notify their line manager or Director of Information and Innovation if they know or suspect a conflict of this policy has occurred or may occur in the future. This includes notification of any actual or suspected data security breech
- familiarise themselves with the following code and guidance documents which form the basis of the mandatory Confidentiality and Information Security Training and are available on the Intranet: *Information Management and Security Guidance suite of documents*

4. Definitions

Personal data – any information relating to an identified or identifiable natural person ('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. This includes information stored electronically, or on paper.

Data subject – any living individual who is the subject of personal data held by an organisation.

Data controller – the public authority, alone or jointly with others, that determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Processor- (CSW) the organisation conducting the "processing" activities on behalf of the data controller.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject. CSW, as data processor will support the Controller in this activity.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child – the GDPR defines a child as anyone under the age of 16 years old. The processing of personal data of a child under 13 years of age is only lawful if parental or custodian consent has been obtained.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

5. Processing Personal Data

CSW processes personal data (including special categories of personal data) in accordance with our obligations under Data Protection and GDPR Regulations and we so only in accordance with meeting one of the legal conditions for processing data. These are:

1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

3. processing is necessary for compliance with a legal obligation to which the controller is subject;

4. processing is necessary in order to protect the vital interests of the data subject or of another natural person;

5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child

We use personal data for:

- performing a contract (or services) between us;
- complying with any legal obligation; or
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing.

The legal basis under which we are processing data will vary according to our relationship with you and in some instances we will be acting as the data processor on behalf of another organisation that is the data Controller. In all cases we will inform you of the legal basis that we intend to rely on for processing your information, or ensure that the Controller for whom we are processing data has ensured you have been information. We will never use personal data for purposes other than for that it was collected.

Sharing personal data

We will share relevant personal information with contractors, partners, clients and customers in pursuance of effective delivery of our legitimate business activities

We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions and those issued by the Data Controller.

6. Data Processor and Data Controller obligations

Within the Data Protection Legislation there are two key roles; Data Controller and Data Processor.

CSW operates as the Data Processor for a range of contractors, including but limited to the Local Authorities, the Skills Funding Agency and the Big Lottery, whilst they retain the role as Data Controller. Therefore each contract and business activity requires a different approach and set of processes to meet the requirements of the respective Data Controller and Processor. This particularly relates to meeting the requirements of processing Data Subject Access Requests {DSAR} and Data Breaches.

7. Data Breaches

We have robust measures in place to minimise and prevent data breaches from taking place. However, should a breach of personal data occur this will be documented on our Incident Management recording system, in line with our Reporting Information Related Incidents and the data controller notified. If the breach is likely to result in a risk to the rights and freedoms of individuals then we will also notify the Information Commissioner's Office within 72 hours**.**

8. Data Subject Rights

Data subjects have rights regarding data processing, and the data that is recorded about them. This is defined by the Data Controller who determines the legitimacy for processing. These rights include the right to:

a. know the information about what personal data we process, how and on what basis as set out in this policy.

b. to access their own personal data by way of a subject access request (see below).

c. to correct any inaccuracies in their personal data.

d. to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected.

e. to object to data processing

f. to receive a copy of your personal data and to transfer your personal data to another data controller.

g. to be notified of a data protection breach concerning your personal data.

9. Subject Access Requests (SARs)

Individuals (data subjects) have the right to access their personal data held by CSW upon their request. All SARs will be dealt with in accordance with our Subject Access Procedure.

In the role of data processor CSW will support the Data Controller and action requests made by them in response to SARs that they receive.

Where a SAR is received directly from the individual, they will be referred to the Data Controller, or details taken and passed on to the Data Controller, whichever method is preferred by the data subject.

Such requests from individuals or their representatives should be referred to Director of Information and Innovation.

10. Consent

CSW Group understands 'consent' to mean explicit and freely given by the data subject and that they have been fully informed of the intended processing and have signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them.

The consent of the data subject can be withdrawn at any time.

Decisions on a young person's ability to give consent will be based on the Fraser Guidelines. This means that their consent must have been fully informed and freely given.
See www.britishcouncil.org/governance/jusrig/human/childrig/cr02a.htm
www.butterworths.co.uk/academic/fortin/cases/853_0402.htm

The consent of the individual data subject must be obtained before their personal information can be shared with a third party organisation or individual.

The explicit consent of the individual data subject must be obtained before sensitive personal information is processed or shared.

Exceptions to this are where there is a contractual requirement (e.g. with Local Authority contracts); or where there is a legal requirement or duty to disclose information; or where there is a risk of serious harm or threat to life or to national security.

11. Data Security and Risks

All employees and volunteers are responsible for ensuring that any personal data which CSW holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by CSW to receive that information and has entered into a confidentiality agreement.

All employees and volunteers are required to act in compliance with our Data Protection and Information Security Procedures to ensure the security of personal, sensitive and confidential information held by CSW.

CSW recognises that there are risks associated with processing personal information. Where a type of processing, is likely to result in a high risk to the “rights and freedoms” of natural persons, CSW Group shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (Data Protection Impact Assessment-DPIA). This will be in line with the DPIA procedure and documented through our Risk Management System. Where a decision is made to proceed, appropriate controls will be implemented to reduce the level of risk associated with processing the individual data to an acceptable level and in line with GDPR requirements.

12. Data Retention and Disposal

CSW will only retain personal information only for as long as is necessary for legal or regulatory reasons or, for legitimate organisational purposes, in line with the Document Retention Policy and Document and Record Retention Schedule. Personal data will only be disposed of in a way that protects the “rights and freedoms” of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and in line with the Information Security Destruction and Disposal Procedure.

11. Complaints

Individuals who wish to make a complaint relating to a breach or how their personal data is being processed can contact:

Andrew Tellam – Director of Information and Innovation
CSW Group
Poseidon House
Neptune Business Park
Cattedown
Plymouth
PL4 0SJ

Email: DataProtection@cswgroup.co.uk

Or alternatively can contact any member of staff in line with CSW's Complaints Policy.

12. Review and Approval

This policy is reviewed annually as a minimum and approved by the Chief Executive.

Paul Hobson
Chief Executive