Data Protection Policy

CSW Group's data protection policy states the company's commitment to protecting personal data and how it implements that with regards to the collection and use of it. It sets out how it complies with the Data Protection Act 2018 (DPA), which implements General Data Protection Regulations (GDPR) and how it protects the "rights and freedoms" of individuals whose information CSW collects to deliver its services. To support this commitment, CSW has developed, implemented and continuously improves its information management system (IMS).

General Data Protection Regulation

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. Data 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.

In addition, there is an accountability principle which requires an organisation to take responsibility for what it does with personal data and how it complies with the other principles as well as taking appropriate measures and keeping records to demonstrate compliance.

The regulation also states the Rights of the Individual must be upheld. This is dealt with in Paragraph 8.

More information on the DPA and GDPR can be found directly from: www.ico.gov.uk

1. CSW Data Protection Policy Statement

CSW is committed to complying with data protection legislation and good practice including:

a. developing, implementing and continually improving an IMS to enable this policy to be implemented;
b. processing personal information fairly and lawfully;
c. processing personal information only in order to meet our legitimate operational needs whilst fulfilling legal requirements;
d. collecting only the minimum personal information required for these purposes and not processing excessive personal information;
e. only processing relevant and adequate personal information;
f. keeping personal information accurate and, where necessary, up to date;
g. maintaining an inventory of the categories of personal information processed and establishing appropriate retention periods for this;
h. retaining personal information only for as long as is necessary for legal or regulatory reasons or, for legitimate organisational purposes;
i. keeping all personal information secure;

j. 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
k. supporting the data controller in their role in providing clear information to individuals about how their personal information will be used and by whom;
l. only transferring personal information outside the EU in circumstances where it can be adequately protected;
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. the identification of workers with specific responsibility and accountability for the IMS;
p. ensuring that a nominated lead is responsible for data protection compliance and is the point of contact for all data protection issues;
q. 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;
r. ensuring that queries about data protection, internal and external to the organisation, are dealt with effectively and promptly;
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, temporary staff and subcontractors of CSW. A breach of the GDPR, DPA or this IMS may be dealt with under CSW's disciplinary policy and could also be a criminal offence. In this instance it will be reported to the appropriate authorities.

Partners and third parties working with or for CSW that have access to personal information, will be expected to read and comply with this policy. They will also be required to enter into an agreement which includes standard data protection clauses that they are required to adhere to.

3. Responsibilities

Chief Executive has overall responsibility for compliance with the data protection legislation and this policy.

The Data Protection Officer acts on behalf of the Chief Executive, and for oversight of all issues relating to Data Protection.

Information Systems Relationship Manager is the Data Protection Lead and is required to:

- be the point of contact for all data protection matters within CSW;
- advise staff on any queries they may have;
- be the liaison point for any data breaches;
- closely liaise with the Data Protection Officer;
- maintain and improve compliance with data protection laws;

- maintain the organisation's registration with the Data Protection Registrar.

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

- adhere to the GDPR, DPA and CSW data protection principles in their handling and recording of personal information, whether electronic or hardcopy;
- 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;
- notify their line manager or the Data Protection Officer 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 breach.

4. Definitions

Personal data – any information relating to an identified or identifiable natural person ('data subject'). This includes information stored electronically, or hard copy.

Special category personal data - Personal data which is more sensitive and so needs more protection, including information about a living individual's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics
- Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes
- Health – physical or mental
- Sex life or sexual orientation

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;

Processing – any operation or set of operations which is performed on personal data such as collection, recording, organisation, structuring, storage etc.

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

Personal data breach –is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure, theft, or unauthorised access, to personal data.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 signifies agreement to the processing of personal data.

Child – DPA 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 through an information society service (ISS) is only lawful if parental or custodian consent has been obtained.

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

5. 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 not 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}, also known as Rights of Access Requests and Data Breaches. *See Paragraph 7. CSW will also operate as a data controller for its own internal operations.*

6. Processing Personal Data

CSW processes personal data (including special categories of personal data) in accordance with our obligations under GDPR and DPA and meeting the lawful conditions for processing data.

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 lawful basis under which we are processing data will vary according to our relationship with you and whether we are acting as the data processor or data controller. In both cases you will be informed of the lawful basis under which your information is processed, either buy us or the data controller. The uses, purposes, and lawful basis will be included in a Privacy Notice.

We will not use personal data for purposes other than for that it was collected.

Sharing your personal data

We will share relevant personal information (as above) 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.

7. Data Breaches

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

8. Data Subject Rights

CSW have measures in place to uphold Data Subject Rights when acting as either Data Controller or Data Processor.

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 it is processed;

b. to access their own personal data by way of a subject access request, also known as rights of access request (see paragraph 9);

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 request the restriction or suppression of their personal data, although this is not an absolute right and only applies in certain circumstances;

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

g. to object to data processing;

h. not to be subject to automated decision making;

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

9. Subject Access Requests (SARs) also known as Rights of Access Requests

Individuals (data subjects) have the right to access their personal data held by CSW. 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.

Requests from individuals or their representatives will be referred to the Data Protection Officer.

10. Consent

As described in section 6 we will process personal data in accordance with the lawful basis in Article 6 of the GDPR. One of the bases is consent - where consent is used as our basis for processing it will be obtained before personal information is shared with a third party organisation or individual.

Where we process special categories of personal data, we will ensure this is processed in accordance with the lawful basis Article 9 of the GDPR. One of the bases is explicit consent. Where explicit consent is used as our basis for processing, it will be obtained before special category personal data is processed or shared.

More information on the processing of special category personal data can be found in our Special Category Personal Data Policy.

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

11. Data Security and Risks

All employees and volunteers are responsible for ensuring the protection and security of personal data which they have access to. This includes not disclosing any information to a third party unless that third party has been specifically authorised by CSW to receive that information.

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 individuals, CSW shall carry out an assessment of the impact of the intended processing (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.

13. Complaints

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

CSW Group
Poseidon House, Neptune Business Park, Cattedown, Plymouth, PL4 0SJ

Email: data.protection@cswgroup.co.uk

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

14. Review and Approval

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

Paul Hobson
Chief Executive

Version	Author	Changes	Review Date	Approval
2.8.2	N Dunn	Version control table added to the end of the document DPO and ISRM role as Data Protection Lead separated Chairman Signature removed	15/07/2020	22/10/2020
2.8.3	N Dunn	Data protection email address changed	23/11/2020	23/11/2020