Information Security & Data Protection Policy

Author	Created By: **Alexis Woolley**	
Effective Date: 05/04/18	Reviewed By: **CCS Team**	Date Reviewed: 28/03/18
Standard: **ISO20121**	Approved By: **CCS Board**	Date Approved: 04/04/18

Revision History

Revision	Date	Description of changes	Requested By
0.0	04/04/18	Initial Release	BT
1.1			
1.2			

Policy: This policy seeks to meet best practice in information security, data protection and all relevant legislation.

Purpose: Its purpose is to safeguard the security and confidentiality of all information, information systems, networks and applications owned or held by Creative Carbon Scotland, in a way that is proportionate to the organisation's size and operations. Implementing this policy will enable CCS to refine and improve current administrative systems.

Scope: This policy applies to all information, information systems, networks, applications, locations and users in all areas of our work. This policy covers personal data relating to CCS employees and to individuals and organisations external to CCS with whom CCS exchanges goods or services.

Related Policies & Procedures:	This policy will affect amongst other things all policies and procedures relating to CCS staff and freelance contractors, relevant individuals outwith CCS, information sharing with project partners and networks, publications in both hard-copy and electronic media and CCS procurement especially relating to electronic communications.
Responsibilities:	The responsibility to ensure compliance with this policy applies to anyone who works or volunteers with Creative Carbon Scotland, including but not limited to: Trustees, Staff, Interns, Freelance or casual staff and volunteers. This also applies to external agencies to whom we send data for processing for business purposes (eg bookkeeper).

Our Policy

Information Security

1. Creative Carbon Scotland (CCS) considers the promotion of information security measures to be a mutual objective for its Trustees, management and staff at all levels. CCS will work to safeguard the security of information it holds in terms of personal privacy and organisational confidentiality, and endeavours to practise a policy of information security.

2. CCS regards the protection of data belonging to its staff and the people it works with as being of prime importance. CCS will attempt to ensure that a high standard of data protection is maintained in the workplace in line with the Data Protection Act 1998, General Data Protection Regulation (EU) 2016/679 and other relevant legislation.

3. Any contractual arrangements into which CCS enters that involve people or organisations outwith CCS being given access to the data CCS holds, must require that such contractors comply with this policy.

4. Anyone working with or for Creative Carbon Scotland should report any risks to information security, whether immediate or long term, to their line manager and their line manager should respond within 10 working days with information about how the risk is being mitigated. If the matter is not resolved it should be reported to the Convenor.

5. It is CCS policy that all IT devices used for CCS business be password protected, but nevertheless, in the event that any IT device containing personal data is stolen or lost, CCS will inform the Information Commissioner's Office immediately.

6. At the end of any term of employment, anyone who has been working with or for Creative Carbon Scotland must be prepared to demonstrate that any data processed by them on behalf of CCS during their employment has been removed from their personal devices.

Data Protection

7. Employees' attention is drawn to the Eight Principles of Data Protection, which state that as an employee you have legal duties to ensure that personal data is:
   - used fairly and lawfully
   - used for limited, specifically stated purposes
   - used in a way that is adequate, relevant and not excessive
   - accurate
   - kept for no longer than is absolutely necessary
   - handled according to people's data protection rights
   - kept safe and secure
   - not transferred outside the European Economic Area without adequate protection.

   Note that there is stronger legal protection for more sensitive information, such as:
   - ethnic background
   - political opinions
   - religious beliefs
   - health
   - sexual health
   - criminal records.

8. CCS will use a Privacy Notice to let contacts whose personal data we hold know:
   - why we are requesting data (including the specific purpose for which we require the data)
   - what we are going to do with the data
   - how we will protect the data
   - how often we will ask the data owner if they wish CCS to retain or delete the data
   - how the data owner can ask to see, correct or remove the data.

   The Privacy Notice will constitute CCS's legal basis for processing data – that is, by consent and for contractual purposes.

9. CCS will operate a CRM (Customer Records Management) system appropriate to CCS's business requirements. The CCS CRM will contain personal data we consider necessary to our business, all of which we will have the data owner's express permission to hold for specified purposes.

10. CCS will publish on our website material that sets out our approach to information security and data protection, and we will ensure that GDPR-appropriate text is included in standard CCS document templates – for example, event sign-up sheets and employment contracts.

11. CCS will operate a regular audit schedule to ensure that data we hold is current and accurate, with any data deemed as a result to be unnecessary for business purposes deleted immediately.