Third Party Access to Data

1. Scope

Caraline is responsible for ensuring the security of its data processing facilities and other information assets in relation to third parties. This procedure applies to all situations where third parties require access to any of Caraline's data, including all of the following categories of external parties with whom Caraline may have agreements in place:

- Service providers, including managed security service providers;
- Clients and customers;
- Outsourcing suppliers including: facilities, operations, IT systems, data collection and call centers;
- Consultants;
- Auditors;
- Providers of IT systems and services;
- Providers of cleaning, catering and other outsourced support services; and
- Temporary staff, including placement and other short-term appointments.

Caraline is responsible for assessing associated third-party risks according to the category and level of risk involved.

2. Responsibilities

Where there is a business requirement to work with third parties, Caraline is required to enter into a formal agreement regarding information security with all third-party service providers.

The Data Protection Officer ("DPO") and all third-party relationship owners responsible for the aforementioned service categories are required to ensure that formal external party contracts are entered into in line with this procedure. All contracts must implement adequate security controls, delivery levels and service definitions and the DPO and third-party relationship owners are responsible for ensuring that these are properly implemented and maintained by the third party, carrying out risk assessments as and when required by this procedure.

Throughout any transition periods Caraline shall offer the same level of security.

3. Procedure

Caraline shall only grant third parties access to organisational assets, including personal data and other information, once a risk assessment has been carried out and the appropriate systems and controls are implemented.

Risk assessment - step by step

1. Caraline carries out a risk assessment and identifies all risks pursuant to third party access to data.

2. For each third party, the risk assessment shall identify the following:

    - The data and the processing facilities which the third party will have access to;
    - The type of access the third party shall have, whether physical and/or logical, whether on or off-site;
    - The exact location from which the third party will access the data;
    - The value and specific classification of the information which the third party will access;
    - The data to which the third party shall not be granted access and which may need to be secured by additional means;
    - A full list of the third party's personnel who will be or are likely to be involved in the access to data, including partners and external contractors;
    - How the third party's personnel shall be authenticated;
    - How the third party intends to store, process and communicate the data;
    - The impact that inaccurate, incorrect or misleading data shared with the third party would have on the third party;
    - The impact on the third party of a potential inability to access the data when required;
    - How Caraline's Security Incident Management Procedure applies and should be implemented if and when information security incidents take place, which involve the third party;
    - Any legal or regulatory matters regarding the third party that are of note; and
    - How Caraline's stakeholder interests may be affected by any of the decisions made in relation to the third party relationship.

3. All systems and controls implemented by Caraline pursuant to the risk assessment must be according to the GDPR and must be within the power of Caraline.

4. Caraline and the third party agree to implement appropriate controls and Caraline's legal advisors shall draw up a contract, which the third party is required to sign. Amongst the third party's obligations is the requirement that all of its personnel are aware of their obligations pursuant to the contract.

5. When drafting the contract, Caraline's legal advisers are required to consider and include all of the following information security policy matters and insofar as any matters are not included within the contract, must provide a documented reason why they was not included, as well as the requirement under which they were identified as part of the risk assessment:

    - A clear definition and/or description of the service or product provided by the third party and a description of the data and its classification;
    - Training, education and awareness requirements for all third party users;

- Any provisions for the transfer of personnel;
- Responsibilities for the installation of software and hardware, as well as maintenance and destruction;
- A robust and clearly defined process of reporting, including structural requirements, reporting formats and escalation protocols;
- A requirement that the third party adequately resources reporting, monitoring and compliance activities;
- A robust and clearly defined change management process;
- An Access Control Policy, refer to Security Access Policy 92017-G;
- Physical controls, including secure areas;
- Controls against malware;
- Data security incident management;
- Appropriate service and security levels, including what would amount to unacceptable service and security, as well as a clearly defined verifiable criteria of performance and security, monitoring and reporting;
- The right for Caraline to monitor and audit the performance of the third party, for which Caraline may use external auditors, including the third party's processes for change management, identifying vulnerabilities and managing information security incidents, as well as Caraline's right to revoke activities;
- The requirements of service continuity;
- Legal responsibilities and liabilities and how they shall be met;
- Copyright and Intellectual Property Rights protection;
- Systems and controls in relation to subcontractors; and
- Conditions for renegotiation and termination of agreements and contingency plans.

4. Information transfer agreements

When the contract between Caraline and a third party is for the transfer of data or software, the following additional controls must be considered, pursuant to an individual risk assessment:

- How the management of both Caraline and of the third party shall be responsible for notifying transmission, dispatch and receipt of data as well as any associated procedures and controls;
- Systems and procedures for ensuring the traceability and non-repudiation of data;
- The means of data transmission;
- Packaging of data;
- Agreed system of labelling the data;
- The selection of couriers and methods of identification;
- The management of data security incidents;
- Escrow agreements;
- Copyright, data protection and software licensing;
- Technical requirements for recording or reading data or software; and
- Any other systems and controls such the use of cryptography.

5. Managing changes to third party services

Please also refer to Security Access Policy 92017-G

Caraline may need to agree to variations to contracts with third parties, as a result of the following potential changes:

- The service it currently offers;
- The implementation of new systems or applications;
- Updates or modifications to its policies and procedures; and
- Updated systems and controls arising from new risk assessments or data security incidents.

A third party may require changes to its contract with Caraline as a result of the following potential changes:

- New networks and infrastructure;
- New technologies, products or new releases of current products;
- New physical locations;
- New physical services;
- New tools or methodologies;
- New service providers; and
- New suppliers of hardware or software.

If any changes arise, a new risk assessment and review of the selected controls must be carried out. Any changes to the contract based on the introduction of new controls, or the amendment of existing controls must be agreed with the third party and inserted into the contract via an agreed variation.

The DPO and relationship owners are responsible for ensuring that the new controls are implemented and incorporated into review and monitoring arrangements already in place.

6. Document owner

The Clear Comm is the owner of this policy document and must ensure that it is periodically reviewed according to the review requirements contained herein.

The latest version of this policy document dated 20 March 2018 is available to all employees of Caraline on the corporate intranet.

This policy document was approved by Caraline's Board of Trustees and is issued by the Chief Executive Officer ("CEO") on a version controlled basis.

Name of CEO: Brian Holmes Date: 20 March 2018

Change history record

Issue	Description of Change	Approval	Date of Issue
1	n/a	n/a	n/a
2	n/a	n/a	n/a
3	n/a	n/a	n/a