

**ISS.4.11**

**Information Security Standard -  
Data Protection Policy**

## Version History

Version	Date	Author	Comments & Updates
1.00	23-May-2018	Richard Levy	Release Version
2.00	01-Oct-2018	Will Lambert	Release for Public Website and change to contact email address to <a href="mailto:dpo@c2craill.net">dpo@c2craill.net</a>

## Release Control

The following personnel must formally approve the document prior to assigning a non-draft version number.

Prepared by (Name & Title)	Authorised by (Name & Title)	Date Approved for Release
Richard Levy	Human Resources Director and Finance Director	21-May-2018
Will Lambert Information Security Function	Andy Stewart-Wright Data Protection Officer	01-Oct-2018

## Distribution

Version	Distributed to	Date distributed
1	Company Intranet	24-May-2018
2	Company Intranet/Public Website	15-Oct-2018

## Document Review

This Data Privacy Management document will be reviewed each year by the document owner/author following the initial publication. Document to be ratified for publication by the Trenitalia c2c Executive Team.

## Copyright

The copyright in the contents of this document is property of Trenitalia c2c Limited. The contents in whole or part must not be modified, reproduced or disclosed or disseminated to others or used for purposes other than that for which it is supplied, without the prior written permission of Trenitalia c2c Limited. © 2018

# Table of Contents

<b>Version History</b>	<b>2</b>
<b>Release Control</b>	<b>2</b>
<b>Distribution</b>	<b>2</b>
<b>Document Review</b>	<b>2</b>
<b>Copyright</b>	<b>2</b>
<b>Table of Contents</b>	<b>3</b>
<b>1. Introduction</b>	<b>5</b>
<b>2. Scope of the Personal Data Protection Policy</b>	<b>5</b>
<b>3. Legal Obligations</b>	<b>5</b>
<b>4. Principles for Processing Personal Data</b>	<b>6</b>
4.1 Lawfulness, Fairness and Transparency	6
4.2 Purpose Limitations	6
4.3 Data Minimisation	6
4.4 Data Accuracy	6
4.5 Storage Limitations	6
4.6 Integrity and Confidentiality (Security)	7
4.7 Accountability	7
<b>5. Enforcement</b>	<b>7</b>
<b>6. Processing Personal Data</b>	<b>7</b>
6.1 Lawful Basis for Processing	7
6.2 Processing Sensitive Personal Data	8
6.3 General Colleague Guidelines	9
6.4 Personal Data Storage (Paper)	9
6.5 Electronically Stored Personal Data	9
6.6 Data Use	10
6.7 Ensuring Data Accuracy	10
<b>7. Data Subject Access Rights</b>	<b>10</b>
I. Right to be Informed	10
II. Right to Rectification	11
III. Right to Erasure	11
IV. Right to Restrict Processing	11

---

V. Right to Data Portability	11
VI. Right to Object	12
VII. Right of Access	12
VIII. Rights in relation to automated decision making	12
<b>8. Colleague Monitoring</b>	<b>12</b>
<b>9. Disclosure to Law Enforcement</b>	<b>13</b>
<b>10. Disclosure to Third Parties Working On Our Behalf</b>	<b>13</b>
<b>11. Sending Personal Data Out of the EEA</b>	<b>13</b>
<b>12. Confidentiality of Processing</b>	<b>13</b>
<b>13. Security of Personal Data</b>	<b>14</b>
<b>14. Data Protection Control</b>	<b>14</b>
<b>15. Compliance</b>	<b>14</b>
<b>16. Reporting Incidents</b>	<b>14</b>
<b>17. Who to Contact About This Policy</b>	<b>15</b>
<b>Glossary</b>	<b>16</b>

## 1. Introduction

The processing of Personal Data is fundamental to our business. As part of its social and legal responsibilities, c2c is committed to protecting personal data. At c2c, we believe the principles of data protection are the foundation on which we build trustworthy relationships with our Customers, Colleagues, Suppliers and Vendors, and the reputation of c2c as a responsible organisation.

All processing is carried out in accordance with the [Privacy and Cookies Notice](#) published for Customers on [www.c2c-online.co.uk](http://www.c2c-online.co.uk) and for Colleagues in the [Colleague Privacy Notice](#).

This Policy is designed to promote consistent standards and practices in handling Personal Data across the business. This requires those who collect and use Personal Data to be transparent about how it is used, to follow the principles on Data Protection and to respect individuals' rights.

## 2. Scope of the Personal Data Protection Policy

This Policy applies to all c2c Employees, Community Volunteers, Consultants, Contractors, Suppliers and Vendors hereinafter to be referred to as: "Colleagues" who store, control and process data (both electronic and physical/paper based) relating to identifiable individuals - Data Subjects.

Information pertaining to data subjects can take the form of Personal Data. Personal Data can include but is not limited to;

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Online Identifiers (ID Address, Cookies, RFID Tags)
- The aggregation of subsets of data relating to the identification of an individual
- Any information relating to an individual

## 3. Legal Obligations

At c2c we are required to comply with the following laws when processing Personal Data (referred to as DP Laws).

- Regulation (EU) 2016/679 (General Data Protection Regulation), as transposed and implemented by:
  - **The Data Protection Act 2018**, and
- The Privacy and Electronic Communication Regulations 2003 and 2011

## 4. Principles for Processing Personal Data

When processing personal data, the individual rights of the data subjects must be protected through adherence to the principles of Data Protection, as set out below:

### 4.1 Lawfulness, Fairness and Transparency

*The personal data shall be processed lawfully, fairly and in a transparent manner.* Data Protection laws require that c2c provides the data subject with information about how their personal data is processed in a concise, transparent and intelligible manner. This must be easily accessible using clear and plain language. Transparency is achieved by keeping the individual informed of the processing activities and data we hold about them. Data Subjects must be informed before data is collected and where any subsequent changes are made.

### 4.2 Purpose Limitations

*Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.* Processing personal data is only permissible if and to the extent that it is compliant with the original purpose for which data was collected. Processing "for another purpose" requires further legal permission or consent.

### 4.3 Data Minimisation

*Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.* We must all ensure that we only personal data which is necessary for each specific purpose (but no more than needed) is collected and processed, in terms of the;

- amount of personal data collected
- the extent of the processing
- the period of storage and accessibility.

### 4.4 Data Accuracy

*Personal data shall be accurate and, where necessary, kept up to date.* Personal data must be accurate and kept up to date. Inaccurate or outdated data should be deleted or amended. c2c are required to take "every reasonable step" to comply with this principle.

### 4.5 Storage Limitations

*Personal data shall be kept in a form which permits identification of data subjects for no longer that is necessary for the purposes for which the personal data are processed.* Once you no longer need

personal data for the purpose for which it was collected, you should delete it unless you have other grounds for retaining it. A regular review process must be in place with methodical cleansing of data.

## 4.6 Integrity and Confidentiality (Security)

*Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.* Personal data must be protected against unauthorised access using appropriate organisational and technical measures. At c2c, we assess risk, implement protective security controls and, review on a regular basis that our security controls are effective. To comply with Data protection Laws, c2c has a Incident Response Plan in the event of a data breach.

## 4.7 Accountability

*c2c and all c2c Colleagues shall be responsible for, and be able to demonstrate compliance with data protection laws.* c2c must be able to demonstrate compliance with the Data Protection principles. This includes but is not limited to:

- Documenting, maintaining and updating the c2c personal data inventory;
- Documenting, maintaining and updating the c2c privacy notices;
- Documenting the obtainment of appropriate consents;
- Using appropriate organisational and technical measures to ensure compliance with the data protection principles; and
- Where appropriate, using Data Protection Impact Assessments.

## 5. Enforcement

In the UK, Data Protection Laws are enforced by the UK's Supervisory Authority, the Information Commissioner's Office (ICO). All complaints from the ICO or any other Supervisory Authority must be sent to the c2c Data Protection Officer ([dpo@c2craill.net](mailto:dpo@c2craill.net)) immediately.

## 6. Processing Personal Data

### 6.1 Lawful Basis for Processing

Collecting, processing and using personal data, regardless of whether the data is from a Customer or an Colleague, is permitted only under the following legal basis:

#### **Contractual Necessity**

Personal data may be processed on the basis that such processing is necessary in order to enter into or perform a contract with a data subject.

### **Compliance with Legal Obligations**

Personal data may be processed on the basis that c2c has a legal obligation to perform such processing.

### **Vital Interests**

Personal data may be processed on the basis that it is necessary to protect the "vital interests" of the data subject (this essentially applies in "life-or-death" scenarios).

### **Public Interest**

Personal data may be processed on the basis that such processing is necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest, such as the Police or the ICO.

### **Legitimate Interests**

Personal data may be processed on the basis that the controller has a legitimate interest in processing those data, provided that such legitimate interest is not overridden by the rights or freedoms of the affected data subjects.

### **Consent**

Personal data may be processed on the basis that the data subject has consented to such processing.

A legal basis is also required if the purpose of collecting, processing and using personal data if it is to be changed from the original purpose.

**For any other purposes not in the c2c Privacy Notices, guidance must be sought from the Data Protection Officer before collecting any personal data. This will enable c2c to ensure we collect the data in a legal manner, whilst upholding these principles of Data Protection.**

## 6.2 Processing Sensitive Personal Data

Below are the classes of personal data which are considered to be "sensitive":

- Information relating to race
- Information relating to ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health data
- Data concerning sex life or sexual orientation



## 6.3 General Colleague Guidelines

- Access to personal data will be controlled using Role Based Access Control (RBAC) and on a Need to Know basis;
- c2c will provide training to all Colleagues to help them understand their responsibilities when handling personal data;
- Colleagues will keep all data secure, by taking sensible precautions and following the Data Protection Principles in this Policy;
- Personal Data should be regularly reviewed and updated if it is found to be out of date or incorrect;
- Where Personal Data is no longer required, it should be deleted and disposed of in accordance with the [Data Retention, Media Destruction and Backup Policy](#);
- Colleagues should request guidance from the Data Protection Officer if they are unsure about any aspect of data protection.

## 6.4 Personal Data Storage (Paper)

These rules describe how and where data should be safely stored:

- When not required and/or not being used, the paper files should be kept in a locked drawer or filing cabinet.
- Colleagues should make sure paper is not left where unauthorised people could see or access is, like on a printer, fax or photocopier.
- When no longer required, paper records bearing CONFIDENTIAL/INTERNAL protective marking must be shredded or placed into the PHS Data Shred Bins.

Please notify the Data Protection Officer immediately if your business area does not have lockable paper file systems or PHS Data Shred Bins.

## 6.5 Electronically Stored Personal Data

When data is stored electronically, it must be protected from cyber attack:

- Data should be protected by strong passphrases. The [Acceptable User Agreement](#) provides guidance on suitable passphrases.
- If the data is stored on removable media (e.g. DVD, USB sticks, etc...), these must be encrypted and kept locked away when not in use. The [Acceptable User Agreement](#) provides guidance on Removable Media.
- Personal Data should only be stored on designated drives and servers, and should only be uploaded to approved cloud services.

## 6.6 Data Use

When Personal Data is accessed and used it is at the greatest risk of loss, corruption or theft. Therefore the following precautions must be adhered to when using personal data:

- When working with personal data, Colleagues should ensure the screens of their computer are always locked when left unattended.
- Personal data should always be shared on a “Need to Know” basis and encrypted before being shared electronically. The Data Protection Officer or a member of the Information Security Function (ISF) can provide guidance on how to do this for authorised external contacts.
- Personal Data should never be transferred outside the European Economic Area (EEA) without the express approval of the Data Protection Officer.
- Colleagues will not save copies of c2c personal data to their own computers and devices.

## 6.7 Ensuring Data Accuracy

It is the responsibility of all Colleagues who work with Personal Data to take steps to ensure it is kept as accurate and up to date as possible:

- Personal Data should not be duplicated. Any duplicates of data that is not required must be deleted.
- We must take every opportunity to ensure data is updated. For example, by confirming a Customer’s details when they contact us by phone or email. If a Customer can no longer be reached on their recorded contact information, it should be removed from the database.
- Retention of personal data will be in accordance with the [Data Retention, Media Destruction and Backup Policy](#).

# 7. Data Subject Access Rights

Individuals, be they current or former Customers or Colleagues, have specific rights under Data Protection Laws. You **must** notify the Data Protection Officer immediately if you get a request from an individual who wishes to exercise one of their below rights:

## I. Right to be Informed

All individuals have the right to be informed of how we collect and use their data. This is typically done through the c2c [Privacy and Cookies Notice](#) and the [Colleague Privacy Notice](#).

## II. Right to Rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. We have an obligation to correct the inaccuracies and to respond to the request within one month.

## III. Right to Erasure

The right to erasure is also known as 'the right to be forgotten'. This right enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

However, the right to erasure does not provide an absolute 'right to be forgotten'. Certain records must be kept under Statutory Law and regulations. The [Data Retention, Media Destruction and Backup Policy](#) has full details of different record types and lengths of time they will be kept for, however the following types of documents provide a brief example of records required to be kept;

- Financial Records - 7 Years
- Health Information - upto 40 years

Individuals have a right to have personal data erased and to prevent processing in some specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data has to be erased in order to comply with a legal obligation.

## IV. Right to Restrict Processing

Individuals have a right to 'block' the processing of their personal data. If we receive such a request we must ensure that we retain just enough information to the restriction is respected in the future.

## V. Right to Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows the individual to move, copy or transfer their personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

## VI. Right to Object

Individuals have the right to object to c2c processing their personal data based on legitimate interests and/or direct marketing (including profiling).

## VII. Right of Access

All individuals who are a subject of personal data held by c2c are entitled to:

- Obtain a confirmation of the processing;
- Be informed the Personal Data we hold about them;
- Be informed of the categories of Personal Data concerned, and
- Obtain a copy (subject to certain limitations and exemptions).

## VIII. Rights in relation to automated decision making

Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal (or similarly significant) effects concerning the individual without any human intervention (eg automatic refusal of an online credit application or decisions on recruitment).

c2c does not make any decisions about an individual solely on the basis of automated decision making.

If an individual contacts c2c requesting the execution of any of these rights, the individual should be asked to email [sar@c2craill.net](mailto:sar@c2craill.net) to make a subject access request.

- Under Data Protection Laws we must respond to valid requests within no more than one month.
- For more info, please see the [Subject Access Request Policy & Guidance](#), or by email at [dpo@c2craill.net](mailto:dpo@c2craill.net).

## 8. Colleague Monitoring

c2c may undertake the monitoring of Colleagues in the workplace to protect the commercial interests of the business, to ensure a safe working environment for all Colleagues, for the prevention and detection of crimes and to comply with legal obligations (e.g. subject access requests). Monitoring of Colleagues can be carried out by:

- Recording using CCTV Cameras
- Viewing company emails
- Manual and automated tracking of emails
- Recording logs of websites visited
- GPS/Geolocation tracking of c2c vehicles

**Note:** Disciplinary proceedings may make use of any Colleague monitoring methodologies stated here.

## 9. Disclosure to Law Enforcement

In certain circumstances, the Data Protection Laws allow personal data to be disclosed to law enforcement agencies without the consent of the data subject.

In such circumstances, c2c will disclose requested data. We must ensure the request is legitimate. If you receive such a request, seek assistance from the Data Protection Officer.

## 10. Disclosure to Third Parties Working On Our Behalf

c2c has a process for appointing suppliers to process Personal Data. To onboard a new supply, please contact the Head of Supply Chain or the Data Protection Officer for guidance. A Data Protection Impact Assessment will be completed BEFORE any transfer of data.

## 11. Sending Personal Data Out of the EEA

Data Protection Laws place restrictions on transferring personal data outside of the European Economic Area. Any c2c Colleague must seek guidance and permission from the Data Protection Officer prior to attempting to undertake such action, in order to allow any privacy impacts to be assessed and associated safeguards and mitigation controls can be established.

## 12. Confidentiality of Processing

Colleagues may have access to personal data only as is appropriate for the type and scope of the task required.

Colleagues are forbidden to

- use personal data for private or commercial purposes
- disclose it to unauthorised persons, or
- make it available in any other way.

Line Managers must inform their Colleagues at the start of the employment relationship about the obligations under data Protection. These obligations shall remain in force even after employment has ended.

At all times, the “Need to Know” Principle must be followed.

## 13. Security of Personal Data

We must ensure that the appropriate technical and organisational security measures are in place to safeguard personal data against unauthorised or unlawful processing, including preventing unauthorised access, accidental loss, destruction or damage to personal data.

We should always exercise extreme caution when disclosing Personal Data via any means. In particular, the requesting person's' identity should be checked to ensure the information is only given to those who are legally entitled to it, whether they are inside or outside of the c2c organisation.

**Do not provide any personal information if you are in any way unsure of the requestor's identity.**

Further specific information can be found in the c2c [Identification & Verification Policy and Guidance](#), c2c [Subject Access Request Policy and Guidance](#) and c2c [Data Classification Policy and Handling Guidelines](#).

## 14. Data Protection Control

Compliance with the Personal Data Protection Policy and all applicable Data Protection Laws is checked regularly with data protection audits and other controls. The performance of these controls is the responsibility of the Data Protection Officer and other company compliance teams.

The results of the data protection audits must be reported to c2c's Board of Directors, or individual representatives of the Board. Functional Directors will be responsible for ensuring that the recommendations and conclusions are actioned/mitigated.

## 15. Compliance

c2c has an obligation to comply, and demonstrate its commitment, to all relevant laws and contractual requirements. This Personal Data Protection Policy forms part of the Information Security/Data Privacy suite of policies and is designed to help ensure c2c's information is handled in the most secure manner throughout its lifecycle – from creation to retention and/or destruction.

## 16. Reporting Incidents

If you become aware of any breach or potential breach of this Policy, for example, the loss of Personal Data or attempts to obtain Personal Data by deception, you must immediately report this to the IT Help desk, [IT.HelpDesk@c2craail.net](mailto:IT.HelpDesk@c2craail.net) or phone 0330 380 0667 or directly to the Data Protection Officer.

---

## 17. Who to Contact About This Policy

Any questions about this policy should be directed to the Data Protection Officer.

**Email:** [dpo@c2craill.net](mailto:dpo@c2craill.net)

**Phone:** 0330 109 8130

**Write to:** Data Protection Officer, Trenitalia c2c Limited, 2nd Floor, Cutlers Court, 115 Houndsditch, London EC3A 7BR

## Glossary

Term	Meaning
Colleagues	all c2c Employees, Community Volunteers, Consultants, Contractors, Suppliers and Vendors.
Community Volunteer	A person or organisation that freely provides a service or performs a designated role or activity.
Contractor / Supplier / Vendor / Consultant	A person or organisation that undertakes a contract to provide goods, works, services or tenancy to c2c
Controller	A person, organisation, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Classification:	
<i>CONFIDENTIAL</i>	Highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know. Explicit authorisation by the Data Owner is required for access because of legal, contractual, privacy, or other constraints. Confidential data has a very high level of sensitivity
<i>INTERNAL</i>	Information that must be guarded due to proprietary, ethical, or privacy considerations and must be protected from unauthorised access, modification, transmission, storage or other use. This classification applies even though there may not be a statute requiring this protection. Internal Data is information that is restricted to personnel who have a legitimate reason to access it
<i>PUBLIC</i>	Information that may or must be open to the general public. It is defined as information with no existing local, national, or international legal restrictions on access or usage. Public data, while subject to disclosure rules, is available to all employees and all individuals or entities external to c2c
Data Subject	Is any living person who's personal data is being collected, held or processed.
Employee	A person employed by c2c under a contract of employment (for the avoidance of doubt this includes FTE's and those employed on fixed term contracts, but not those employed through consultancy



	agreements)
Information Commissioner's Office (ICO)	The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
"Need to Know" Principle	The "Need to Know" principle pertains to Protectively Marked Material that Colleagues will need to have access to, or modify in order to carry out their roles within the organisation. Colleagues who do not have "Need to Know" shall be prohibited from accessing and processing such material.
Personal Data	<p>Any information relating to a living individual who can be identified from that information – either on its own or when put together with other information that c2c holds. This includes any expression of opinions about the individual and any intentions of any person in respect of the individual.</p> <p>For example, names, addresses, telephone numbers, CCTV images, photographs, etc.</p>
Processing	<p>Collecting, obtaining, recording or holding the information or data or carrying out an operation or set of operations on Personal Data, including, but not limited to:</p> <ul style="list-style-type: none"> <li>● Organisation, adaptation or alteration of the data</li> <li>● Retrieval, consultation or use of the data</li> <li>● Disclosure of the data by transmission, dissemination or otherwise making it available, or</li> <li>● Alignment, combination, blocking, erasure or destruction of the data</li> </ul>
Role Based Access Control (RBAC)	RBAC is a method of restricting network and application access based on the roles of the individual users within the business. RBAC let's Colleagues have access rights to only the information they need to perform their job role and prevents accessing information that does not pertain to their job role.
Sensitive Personal Data	<p>Includes Personal Data consisting of information relating to:</p> <ol style="list-style-type: none"> <li>1. Racial or ethnic origin</li> <li>2. Political Opinions</li> <li>3. Religious beliefs or beliefs of a similar nature</li> <li>4. Trade Union membership</li> </ol>

---

	<ol style="list-style-type: none"><li>5. Physical or mental health or condition</li><li>6. Sexual life</li><li>7. Commission or alleged commission of any criminal offence</li><li>8. Proceedings for any criminal offence or alleged criminal offence, the disposal of such proceedings or the sentence of any court in such proceedings.</li></ol>
--	--

This page is intentionally blank to indicate the end of this document