## The Cashroom Limited (TCR)

| | |
|---|---|
| **Policy name** | **Data protection policy** |
| **Policy reference** | |
| **Policy owner** | Mike Touhey |
| **Policy writer(s)** | David Calder, Mike Touhey, Rachel Faris, Stuart Lockhart |
| **Policy approver** | Managing Director, Operations Director, Head of Client Services |

## Document control sheet

| Version no. | Approved by | Date | Key changes | Sections affected |
|---|---|---|---|---|
| 1.1 | Mike Touhey | 20/11/2018 | 1st full review<br>Typing errors<br>New Back up policy<br>Changing names to job titles<br>Ensuring consistency between linked sections<br>Matching table of contents and headers | All areas.<br>Specific changes made to;<br>Schedule 2 part 6 (Back up Policy) |

## Changes Log

Key Changes since last Version

| Version no | Change | Reason for Change |
|---|---|---|
| 1.1 | Back up Policy | New back up strategy following change in IT Support Providers |

## Contents

# DATA PROTECTION POLICY

## 1. Policy governance

This policy is owned by the Operations Director.

The policy owner is responsible for ensuring the following:

1.1 That this policy remains up to date.

1.2 That this policy is effectively implemented through appropriate process and procedural development, training and staff communication.

1.3 That any lack of compliance with this policy is appropriately raised and dealt with and that any breaches to the policy, reported by either the business teams or the data compliance team, are addressed and reported as required.

This policy is designed to make clear to The Cashroom's (also referred to as TCR) business teams and their business managers their data protection responsibilities.

1.4 The role of The Cashroom's business teams is to ensure they understand their data protection responsibilities and act in accordance with The Cashroom's data protection policy and procedures.

1.5 The role of The Cashroom's business managers is to ensure the business teams comply with this policy and to report breaches to this policy in accordance with The Cashroom breach procedures. This includes ensuring the business teams have appropriate knowledge of and training in their data protection responsibilities and knowledge of and training in how to raise and report breaches.

1.6 The role of The Cashroom's data compliance team is to ensure it is carrying out effective monitoring to affirm that the standards laid down in this policy are being adhered to by the business teams and where they are not, to raise them as a matter of urgency with the board and any required regulatory authority.

## 2. Background

The purpose of this policy is to articulate The Cashroom's approach to data protection - providing details of the principles, ethos and approach The Cashroom takes to its data protection practices to ensure that it treats its customers and data subjects fairly. It also provides details of how The Cashroom monitors its data protection activities to ensure it is meeting the Information Commissioner's Office (ICO) and other related regulatory standards.

The General Data Protection Regulations (GDPR) are enforceable in the UK from 25 May 2018. The GDPR are based on and builds out from the Data Protection Act 1998 (DPA). This policy is based on this legislation.

It is the responsibility of The Cashroom's employees to ensure that they are complying with the policy. Team Leaders are responsible for ensuring their teams understand and carry out the terms of the policy. It is also the responsibility of the Data Compliance Team in Operations to raise and report any breaches to the operation or application of the policy to the Board.

## 3. Scope

This document covers all aspects of the Cashroom's data protection policy, including physical security, information security and data protection.

Detailed policies covering all aspects of physical security, information security and data protection are included in Schedules to this document. These Schedules are

### 3.1. Schedule 1: Physical Security

3.1.1 Access Control

3.1.2 Clear Desk Policy

3.1.3 Document Storage and Destruction

**3.2. Schedule 2: Information Security**

3.2.1 IT security & compliance policy

3.2.2 Email policy

3.2.3 Email deletion policy

3.2.4 Internet usage policy

3.2.5 Password management and encryption policy

3.2.6 Backup policy

3.2.7 Mobile and remote working policy

3.2.8 Public Wi-Fi policy

3.2.9 BYOD policy

3.2.10 Disposal and destruction policy

**3.3. Schedule 3: Data Protection**

3.3.1 Use of Client Data

3.3.2 Use of Employee Data

3.3.3 Use of Marketing Data

3.3.4 Suppliers Data

3.3.5 Data Protection Impact Assessments

3.3.6 Data Subject Requests

3.3.7 Data Breach Management and Reporting

3.3.8 Data Protection Compliance Monitoring

## 4. Purpose

The Cashroom is committed to collect, manage and store data on its customers and data subjects in a transparent manner that ensures that data is safe, protected and liable to cause no detriment to customers or data subjects.

The Cashroom also understands the importance of designing its products and services in such a way that ensures its customers and data subjects privacy is assured and that they are ‘private by default’. The Cashroom also understands the importance of ensuring data subjects and customers have effective access to their data and can easily and simply request their data be amended or erased where incorrect or inappropriately collected, managed or stored.

This data protection policy is written to be compliant with the General Data Protection Regulation (GDPR). Its purpose is to ensure that there is a usable reference guide to help direct their attitudes and behaviors in relation to the proper collection, management and storage of data as laid out in the DPA and GDPR. It builds specifically on the eight data principles listed in the DPA and the subsequent guidance detailed in the GDPR.

The outcome that this policy is designed to foster is the safe, transparent and effective collection, management and storage of data to ensure the risk of customer and/or data subject detriment is minimised in all The Cashroom’s services, products and activities.

## 5. Policy statement

The Cashroom takes collecting, managing and storing personal data in a transparent, safe and effective manner very seriously.

The Cashroom wishes to ensure that it is effectively collecting and protecting customer and Data Subject data in a manner that minimises the risk of detriment to those parties.

The Cashroom wishes to ensure that its staff have access to this policy and have read and understood its contents and requirements. This is important to The Cashroom as it expects all its staff to comply with the policy and its guidelines.

The Cashroom is committed to developing effective data protection processes and procedures to enact the ethos and standards contained within this policy.

The Cashroom is committed to ensuring that its staff are appropriately informed of and trained in the data protection activities associated with this policy.

The Cashroom is committed to identifying, reporting and remediating any significant breaches to this policy to the data compliance team in Operations, the board and any external regulators as detailed in the guidelines within this policy.

The Cashroom will not tolerate a failure to abide by this policy and will take management action against those who fail to follow this policy and its guidelines.

## 6. Policy standards

The Cashroom data protection policy has the following key policy standards.

### 6.1 Governance.

The Cashroom commits to put in place effective governance arrangements to ensure the management of data protection activities. These include:

6.1.1 Discussion of The Cashroom data protection activities at Board on a Quarterly basis.

6.1.2 The Cashroom has appointed a Data Protection Administrator who has primary responsibility for enforcing this policy.

6.1.3 The development of and approval by the Board of The Cashroom′s data protection policy and associated processes that comply with the GDPR.

6.1.4 The set up and support of a suitable data compliance team to monitor data protection activities and report on compliance with the GDPR to the Board and, if necessary, following a significant breach to ICO, affected individuals and other regulated authorities within the timeframe specified within the GDPR.

### 6.2 Training.

The Cashroom commits to training staff in the operation of this policy, and their responsibilities under the GDPR.

### 6.3 Data protection impact assessments.

Where there is a possibility that The Cashroom will engage in a potentially high risk data processing activity (see GDPR guidelines) then The Cashroom commits to undertake a data protection impact assessment (DPIA).

### 6.4 Lawful basis.

The Cashroom also commits to reviewing, approving and documenting its ‘lawful basis’ for collecting data prior to collecting or processing new data sets

### 6.5 Purpose.

The Cashroom commits to only using the data it collects from data subjects for the purpose(s) it was collected. Further consent will be sought if the data is to be used in a different manner

**6.6 Rights.**

The Cashroom commits to respecting the rights of individuals in relation to the protection of their data as detailed in the GDPR and including:

6.6.1 **The right to be informed**

Where The Cashroom is the Data Controller, when collecting data, it commits to inform individuals of the following:

6.6.1.1 The firm's identity

6.6.1.2 How the firm will use the information

6.6.1.3 The lawful basis under which the data is being collected

6.6.1.4 The duration the data will be retained for

6.6.1.5 The individuals' right to and process for complaining to ICO

6.6.2 **The right of access**

The Cashroom commits to respond to subject access requests:

6.6.2.1 within 40 calendar days of receiving a request

6.6.2.2 Without charge, unless the request is manifestly unfounded or excessive

6.6.2.3 Without refusal unless a clear and compelling reason for the refusal can be provided and details of the process for complaining are provided with the refusal.

6.6.3 **The right to rectification**

The Cashroom will deal with a rectification request within one month of receipt. If the requests are complex or numerous we will advise the Data Subject that we will deal with the request within 2 months, and explain why.

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, we will charge a reasonable fee for dealing with the request, or may refuse to deal with the request. If we do so, we will explain why, and advise the Data Subject of their right to complain and to a judicial remedy.

6.6.4 **The right to erasure**

The Cashroom commits to erase any unwarranted information that it holds within 1 month of it being acknowledged as unwarranted by The Cashroom

6.6.5 **The right to restrict processing**

The Cashroom commits to restrict the processing of any information and, following a complaint, to restrict the processing of any information within 1 month of it being acknowledged as necessary to do so by The Cashroom

6.6.6 **The right to data portability**

The Cashroom commits to provide agreed personal data in a structured commonly used and 'machine readable' form, on request

6.6.7 **The right to object**

The Cashroom commits to ensure that all individuals are provided with details about how to register a complaint with ICO at the time a complaint is raised

6.6.8 **Rights in relation to automated decision making and profiling**

The Cashroom does not use personal data to make automated decisions or complete individual profiling.

**6.7 Consent.**

The Cashroom commits to ensure that, where consent is the lawful reason for processing, all data is collected with appropriate consent. Specifically that when data is collected the consent obtained is:

6.7.1 Specific and granular in nature

6.7.2 Clearly articulated in plain English

6.7.3 prominent within the collection process and documentation

6.7.4 Requires the individual giving consent to opt-in

6.7.5 Properly documented and stored

6.7.6 Easily withdrawn

6.7.7 Not gained from children under the age of 16 without the consent of a parent or guardian

**6.8 Duration.**

The Cashroom commits to keeping its data in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed, or for other lawful reasons

**6.9 Quality.**

The Cashroom commits to keep accurate data and will take reasonable steps to ensure that personal data that is inaccurate with regard to the purposes for which it is processed, is erased or rectified within 1 month of being recognised as such.

**6.10 Information security.**

The Cashroom commits to ensure the appropriate security of the personal data it collects, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage by using appropriate technical or organisational measures. Further details of these policies are contained in the Schedules to this policy.

**6.11 International data.**

The Cashroom commits to the guidelines provided in GDPR and the DPA with regard to sharing data internationally and recognises that the level of protection afforded by GDPR must not be undermined if any personal data is transferred outside of the European Union.

## 7. Policy controls and processes

### 7.1. Monitoring structure

7.1.1 It is the responsibility of The Cashroom's staff (the first line of defence) to ensure that it is enacting and following the policy guidelines and meeting the policy standards.

7.1.2 It is also the responsibility of the first line of defence to raise and report any breaches to the operation or application of the policy to the DPA (dataprotection@thecashroom.co.uk), and the Board.

7.1.3 To support the first line of defence the DPA (the second line of defence) will carry out additional monitoring activities on both a scheduled and unscheduled basis:

7.1.3.1 The scheduled monitoring will take place every 6 months as detailed in the data protection compliance monitoring plan (contained in Schedule 3) and will review the first line of defence's records, documents and knowledge of the data protection arrangements.

7.1.3.2 The unscheduled monitoring is likely to be triggered by a specific incident (e.g. a specific breach) and will review and assess compliance with any relevant aspects of the data protection policy or process.

### 7.2. Reporting procedures

The Cashroom takes seriously the reporting of management information in relation to the carrying out of its data protection activities. In particular it is committed to reporting significant breaches of the regulations to ICO within 72 hours after the breach has come to the attention of TCR staff. The standards for reporting data breaches are contained within the Cashroom's breach management policy (see Schedule 3).

The Cashroom also acknowledges that on occasions it may also need to inform Data Subjects if they are impacted by a data breach and that The Cashroom is committed to ensuring it has the procedures in place to be able to carry this out if required.

The Cashroom expects, that in addition to the normal flow of management information (detailing any data related risks and issues) from the business areas handling data that The Cashroom Board will receive a written report from the data compliance team detailing the risks and issues generated by the monitoring it has completed in relation to The Cashroom's data protection activities. They will receive that report every 6 months.

### 7.3. Policy communication and training

This data protection policy is stored in the GDPR folder on the "Q" drive and can be accessed by all employees.

In addition to the initial post-recruitment training provided by the Operations Team to all staff, The Cashroom commits to provide annual refresher training in data protection for all its staff.

The data compliance team will be asked to provide evidence on the quality and coverage of the requisite training as part of its reports to the board.

## 8. Policy review and update process

Events that will trigger a policy review are detailed below. The DPA will ensure the Data Protection Policy is reviewed, as required.

Standard triggers:

### 8.1 Calendar-based

If no other trigger results in a policy review then the policy will be reviewed on an annual basis.

### 8.2 Business change-based

The policy will be reviewed following changes to business strategy or policies that relate to this policy

Emergency triggers:

### 8.3 Incident-based

The policy will be reviewed as a result of identifying a major issue either during the monitoring process or as the result of an incident or breach that is the outcome of a weakness in the policy

### 8.4 Ad-hoc Improvement based

The policy will be reviewd as a result of a suggestion for an improvement

### 8.5 Regulatory-based

The policy will be reviewed as a result of the implementation of new regulation

### 8.6 Customer sensitivity based

The policy will be reviewed as a result of customer perceptions changing that may require the policy to drive different outcomes or behaviours

# SCHEDULE 1: PHYSICAL SECURITY

## 1. Access Control

### 1.1. Head Office (Livingston)

**1.1.1.** The building is protected by an Intrusion Detection Alarm system which is monitored by an Alarm Receiving Centre. On activation the Alarm Receiving Centre advise the Police, and senior management.

**1.1.2.** Access to the building is via key fob access which is administered by Operations (Livingston).The system records entry of all fob holders. Keys to the premises are held by management and one copy with the cleaning contractor.

**1.1.3.** Visitors must be met at the front door and wait in reception until a member of staff who can verify the visitor's identity is available. If such a member of staff is not available, the visitor must not be allowed to wait in the work area within TCR's office.

**1.1.4.** All staff are responsible for challenging any unauthorised access attempts or unaccompanied visitors they do not recognise and trust.

### 1.2. England & Wales office (Skelmersdale)

**1.2.1.** The Skelmersdale office is part of a managed office, West Lancashire Investment Centre (WLIC). The building security is managed by the WLIC management company with access to the building controlled by a main reception area. All visitors have to sign in/out and must be met at reception by an authorised representative of the organisation hosting the visitor met at reception by a member of staff who can verify the visitor's identity. If such a member of staff is not available, the visitor must not be allowed to wait in TCR's office.

**1.2.2.** Access throughout WLIC is controlled by access key fobs, administered by TCR Operations (Skelmersdale). The system records entry of all fob holders. Keys to the premises are held by management and one copy with WLIC.

**1.2.3.** All staff are responsible for challenging any unauthorised access attempts or unaccompanied visitors they do not recognise and trust.

## 2. Clear Desk Policy

The documents we handle on a daily basis contain confidential information and include highly sensitive data. TCR staff are responsible for maintaining this confidentiality and protecting documents and data from unauthorised access.

### 2.1. All staff are responsible for:

**2.1.1.** Removing all unnecessary items that are not permanent/semi-permanent from their desks including documents, post it notes and rubbish when they are not at their desk.

**2.1.2.** removing all items that are not permanent/semi-permanent from their desks including stationery, ornaments, paper, post it notes and rubbish outside of working hours

**2.1.3.** Maintaining a clear desk when they are working by removing all unnecessary items that are not permanent/semi-permanent from their desks including documents, post it notes and rubbish.

**2.2.** Pedestal drawers have been provided for this purpose and filing cabinets are available for storing personal/sensitive data.

As an aide memoire, all staff should use the following principles or 3 "P"s:

**2.2.1. PLAN –** Start each day with a few minutes of planning so you can organise the documents you need for immediate work. Be mindful to use electronic documents rather than paper documents and consider whether you really do need to print a document.

2.2.2. **PROTECT –** When you leave your desk to attend meetings or take a break, remember to lock your computer screen and also remove/store any items as described above.

2.2.3. **PICK UP –** At the end of each day, don't leave documents on or around your desk. It is essential to shred, file or lock up your documents and clear your desk as described above.

## 3. Document Storage and Destruction

TCR has a clear desk policy and all paper, containing personal data, in our office should be stored, when not being used, in a securely locked drawer until its purpose is served. Afterwards documents containing personal data should be destroyed. All members of staff are responsible for placing their own paper, containing personal data, in the secure receptacles. The shredding is handled by a secure commercial shredding company.

# SCHEDULE 2: INFORMATION SECURITY

## 1. IT security & compliance policy

### 1.1. Definition

The purpose of this section is to document the IT security controls for ensuring the integrity, confidentiality, availability and accountability of relevant IT applications and infrastructure. It is our aim to ensure that good industry practice is adopted and followed in relation to IT Security & Compliance.

Our Organisation is designed to deliver high quality customer service to our clients whilst ensuring this is delivered efficiently and effectively with clear accountabilities established for customer service and process effectiveness.

We source our IT from high quality, industry aware vendors who are contracted to deliver secure, available and performing systems. We operate our client systems in line with the client policies and standards.

### 1.2. Roles & Responsibilities

Information security is represented within The Cashroom at a senior level and the Security Management Framework is approved by senior management.

The Operations Director has been appointed as Security Manager. The Security Manager is knowledgeable on security matters and works in conjunction with our IT supplier such that they are able to respond to any client queries and ensure compliance with information security obligations under this agreement. In relation to services provided, the Security Manager acts as a single point of contact for security related matters.

### 1.3. Compliance

1.3.1. We review and document our compliance with this policy by conducting audits of each of the business areas.

1.3.2. The Cashroom has Cyber Essentials Plus accreditation and we undertake an annual risk assessment.

1.3.3. All staff complete regular security awareness training exercises covering the following:

1.3.3.1. Nature of client data and confidential information they have access to

1.3.3.2. Responsibilities in handling client data and confidential information including non-disclosure obligations

1.3.3.3. Requirements for proper handling of client data and confidential information in physical form including transmission, storage and destruction

1.3.3.4. Proper methods for protecting data on client systems, including the use of a password policy

1.3.3.5. Other computer security concerns

1.3.3.6. Workplace security including building access, reporting of incidents and similar issues

1.3.3.7. Consequences of failure to protect information including potential loss of employment, damage to individuals whose private records are divulged and possible civil, financial and criminal penalties.

### 1.4. Communication

Policies and procedures are communicated to all staff on commencement of their employment with the company, following any changes/updates made and periodically as reminders throughout the term of their employment. Appropriate acknowledgement records are maintained. Relevant IT service providers and sub-contractors will also be provided with the IT security & compliance policy. Procedures and acceptance records will also be maintained.

### 1.5. Security Incident Management

If an actual or suspected material security incident has resulted in unauthorised access to, or disclosure of, confidential information, client bank systems or client practice management systems used by The Cashroom personnel then the Data Protection Administrator should be informed. The Cashroom shall make all reasonable efforts to immediately notify clients of such actual or potential security incident, but in any event such notification shall occur within 24 working hours of The Cashroom becoming aware of such Security Incident.

The notification provided shall include at least the following details:

1.5.1 The date of the Security Incident

1.5.2 A summary of all known relevant facts in relation to the Security Incident

### 1.6. Security Assessment

Every year, we instruct a security assessment by an independent third party, with expertise in this area. Accreditation is displayed on our website and we will advise clients of the outcome of that assessment on request. Should our clients wish, they can, at their own expense, instruct a security assessment of our systems on giving 20 days written notice. The frequency, scope and methods used to conduct the security assessment shall be communicated to the TCR Data Protection Administrator, via dataprotection@thecashroom.co.uk for appropriate action, 15 business days prior to commencement of the security assessment.

The Client shall use their reasonable endeavours to ensure that any Client instructed Security Assessment is performed in such a way as to cause as little disruption as reasonably possible to The Cashroom's business. The Cashroom shall provide all assistance reasonably requested by the Client or its Agents in relation to the Security Assessment.

### 1.7. Asset Management

TCR will ensure that a complete and accurate inventory of hardware and software managed by The Cashroom as part of their business (e.g. unique identifiers, version numbers and physical locations) is recorded and kept up to date, and that all Third Party software licensing requirements are met.

The asset owner must notify Operations of the end of the asset lifecycle so that they can arrange for the asset to be disposed of in a safe and secure fashion.

### 1.8. Wireless Access

Access to The Cashroom's systems is subject to authorisation, authentication and encryption protocols consistent with good industry practice and shall only be permitted from locations approved by the Cashroom.

### 1.9. Malware

The Cashroom has established and maintains up-to-date protection against malicious code throughout The Cashroom's business through the use of firewalls and up to date patching.

The Cashroom protects against transferring malicious code to Client systems, Client customers and other Third Parties using Client systems using at least the current industry standard methods.

### 1.10. Firewalls

All traffic networks accessing The Cashroom's network are routed through a firewall. These firewalls ensure secure connections between internal and external systems and are configured so as to only allow the required traffic to pass through.

### 1.11. Emergency Fixes/Updates/Patches

TCR ensures that emergency fixes are approved and implemented when made available, unless this introduces greater business risks. In these cases, TCR will identify how it needs to manage these risks and will schedule the implementation of the fix accordingly.

All changes must be undertaken in accordance with TCR's change management process.

### 1.12. System Design

We identify and implement controls consistent with good industry practice for all TCR systems and networks to protect the confidentiality, integrity and availability of the systems.

### 1.13. Host and Network Device Configuration

TCR ensures that host systems and network devices combining to form TCR's systems are configured to function in accordance with good industry practice, applicable specifications and functionality requirements, and to prevent unauthorised or incorrect updates being applied to such systems and network devices.

### 1.14. Time Synchronisation

Key systems and devices comprising TCR's systems have the correct and consistent time. This is done through synchronisation with a public time server which covers all internal and external PC's once connected to the secure TCR domain.

### 1.15. Workstation Configuration and Remote Working

TCR ensures that, in accordance with good industry practice, workstations connected to the applications and systems forming part of TCR's network and all personal computers used by TCR personnel working in remote locations, shall be configured securely to prevent unauthorised access or changes to data, and protected by physical controls.

### 1.16. Remote Access and Maintenance

Systems security restricts remote access to TCR's systems to authorised individuals only, confined to individual sessions

### 1.17. Resilience

We ensure that all elements of the Cashroom's systems are run on robust, reliable hardware and software located at a tier one data centre facility.

### 1.18. Intrusion Detection

In accordance with good industry practice, TCR deploys intrusion detection tools in our systems to identify and respond to suspected or actual attacks.

### 1.19. Network Design

TCR's network is designed and implemented to cope with current and predicted levels of traffic and shall be protected using all available in-built security controls

### 1.20. Network Documentation

TCR's network for the provision of client services is supported by accurate, up-to-date diagrams that include all system components and interfaces to other systems, and is supported by documented control requirements and procedures. These procedures are held by our IT provider.

## 2. Email policy

### 2.1. Scope

This policy applies to the use of Cashroom email accounts (@thecashroom.co.uk) for business and personal use on Cashroom and non-Cashroom premises including from home and via portable media.

Personal email accounts should not be used to access TCR business applications or platforms.

### 2.2. Compliance

All staff are expected to comply with this policy.

Any breaches of this policy may result in a member of staff's employment or association with the Cashroom being terminated. It may also result in disciplinary, civil or criminal proceedings.

### 2.3. Responsibility

All managers and Team Leaders are responsible for ensuring that the staff they manage are aware of this Email policy and their individual responsibility for complying with it. They should ensure their staff are equipped to fulfil those responsibilities; this will include covering it at their induction and by identifying and meeting specific and generic training needs through personal development plans.

### 2.4. Legal Requirements

The use of email must comply with the law such as the General Data Protection Regulation (GDPR) (EU) 2016/679 and the associated TCR policies and procedures.

Users must not use email for any purpose that conflicts with their contract of employment.

Users must not agree to terms or enter into contractual commitments or make representations by email without having obtained the proper approval. (A typed name at the end of an email is just as much a signature as if it had been signed personally.)

Email messages have the same legal status as other written documents and must be disclosed in legal proceedings if relevant to the issues.

The content of any emails may be dis-closable under the General Data Protection Regulation (GDPR) (EU) 2016/679 and Freedom of Information Act 2000.

Improper statements may result in the Cashroom and/or user being liable under law.

### 2.5. Security

All passwords and log in details for email systems must be kept confidential. Sharing passwords or log in details will be considered misconduct.

Email attachments that contain personal data must adhere to the “Sending Information to Clients Policy”.

Any computer that is used for work purposes must be installed with up to date, approved anti-virus software.

Portable devices, including mobile and smart phones, used to store emails must be password protected.

### 2.6. Personal use

Reasonable use of personal emails is allowed within The Cashroom, these emails should be stored in a folder marked personal.

If it is necessary to use email for personal communications they must be brief, must not contain attachments, must be carried out in the user’s own time, must not detract from the user’s work duties and must not disrupt the work of others.

### 2.7. Users must not:

2.7.1. Create, hold, send or forward emails that have obscene, pornographic, sexually or racially offensive, defamatory, harassing or otherwise illegal content. (If you receive such a message you should report it to IT@thecashroom.co.uk immediately.)

2.7.2. Create, hold, send or forward emails that contain statements that are untrue, inaccurate, misleading or offensive about any person or organisation.

2.7.3. Access and use another user’s email account

2.7.4. Send or forward chain letters or other similar non-work related correspondence.

2.7.5. Use email for political lobbying.

2.7.6. Knowingly introduce to the system, or send, an email or attachment, containing malicious software (e.g. viruses).

2.7.7. Forge or attempt to forge email messages.

2.7.8. Use instant messaging services (e.g. Microsoft Messenger).

### 2.8. Monitoring

The use of email is not private. The content of email is not routinely monitored but the Cashroom reserves the right to access, read, print or delete emails at any time.

No one has a right of access to an email account. The inappropriate use or abuse of email may result in access being withdrawn or amended.

### 2.9. Liability

The Cashroom will not be liable for any financial or material loss to an individual when using email for personal use or when using personal equipment to access work email.

E-mail correspondence shouldn't embarrass the company or make the company liable for any fines.

### 2.10. Reporting incidents

Users must report incidents of unacceptable use of email to their line manager. The line manager must then report this to the Operations Director.

## 3. Email deletion policy

The Law Society of England and Wales and the Law Society of Scotland require us to keep financial data for 6 full financial years and the current year for audit purposes.

We will apply a 7 year email deletion policy across all mailboxes to comply with these regulations. Any information that has entered the business in email form and is required to be kept for a longer time period, for any reason, will need to be saved in the file structure (Q: Drive).

## 4. Internet usage policy

TCR has a strict policy against unauthorised or inappropriate use of internet services or content. It is to be remembered that information found on the internet cannot always be trusted, and therefore may only be used for business purposes after its authenticity and correctness has been verified. Staff must remain vigilant of potential scams and other fraudulent activity in line with the company's "Social Engineering Policy". Internet access may be monitored for network management and security reasons.

Web browsing is a common method of attack for criminals to try to infect computer systems with malicious code or fool employees into revealing sensitive information. When using company devices, users may only access the internet via the company network where suitable firewall protection is deployed. Users shall not seek to bypass the company's firewall controls via mobile tethering, modems, Wi-Fi or other such direct access unless otherwise instructed or authorised by senior management and in line with the "Public Wi-Fi Policy".

Company devices are only used for internet access if they have the following installed:

- Vendor supported Operating Systems that are patched up-to-date
- Up-to-date malware protection software paired with the latest virus definition files that are configured for on-access scanning of all files including those being downloaded from the internet
- Correctly configured personal firewalls – set to block unsolicited inbound traffic. The company reserves the right to block access by individuals and/or groups to chosen internet web pages where it deems necessary. If access is required to such sites for work-related activity, then a written request shall be submitted to Operations with the relevant senior management authorisation. Under no circumstances must the user seek to circumvent the company's controls and browse unauthorised web pages when using company equipment and/or company networks. Users of company-owned laptops and mobile devices may only connect to the internet after they have been instructed by a member of Operations and after authorisation from senior management in line with the "Mobile and Remote Working Policy". Users of such equipment are responsible for responding to any system alerts and applying

updates where necessary - or informing TCR IT Support to help rectify the issue before continuing to use the system(s).

Users who are authorised to connect to the internet from remote locations – and therefore not protected by the company's firewalls – shall only visit websites that relate to work activity. Users should be extra vigilant and check that the web address/URL is as expected and the address starts with https, where appropriate.

Employees that post messages on social networks, forums, etc., where The Cashroom is referenced, must unambiguously state that their messages do not represent the organisation's viewpoint.

Users must advise Operations when there is no longer a need to have a business online account, to ensure that it is removed.

### 4.1. Unacceptable use or behaviour

Whilst using company equipment, the user shall not:

4.1.1. Visit internet sites that contain illegal, obscene, hateful or other information commonly thought of as being objectionable and offensive;

4.1.2. Use company user IDs or email addresses when signing up to non-work related portals;

4.1.3. Use the same password on more than one web portal and/or online service. The company's password management tool can be used to generate complex and unique passwords, which combine letters, numbers and symbols;

4.1.4. Create business accounts on web portals without authorisation from Operations;

4.1.5. Upload company information to web portals without authorisation;

4.1.6. Upload any information to websites that may bring the company into disrepute;

4.1.7. Download, run or otherwise accept any software from the internet unless part of an authorised procedure;

4.1.8. Seek to bypass or change the installed anti-malware protection software or any other security mechanism including personal firewall settings;

4.1.9. Browse the internet whilst logged into the computer as an administrator of the device;

4.1.10. Place the company's details, web or email details on any site without prior authorisation as this could potentially bring the company's reputation into disrepute.

As website traffic may be monitored for breach of policy, users must alert their line manager should they:

- Inadvertently visit a suspicious website that they suspect contains malware and/or other harmful elements;
- Inadvertently visit a site that that contains illegal, obscene, hateful or other information commonly thought of as being objectionable and offensive.

The line manager should then inform TCR IT support and IT@thecashroom.co.uk so that any remedial actions can be taken.

## 5. Password Management and encryption policy

### 5.1. Background

This policy governs the appropriate use of cryptographic controls (encryption methods) to protect sensitive information against accidental or malicious disclosure. The company protects its sensitive information, that of its third parties, customers and stakeholders, by use of cryptographic controls wherever there is a legal, regulatory or contractual obligation to do so, or when the disclosure of such information could cause damage to the cash flow or reputation of the company.

### 5.2. Key controls

5.2.1. User passwords are managed using an online Password Manager, providing the ability to generate and retrieve complex passwords stored on an encrypted database.

5.2.2. User terminal access policies force users to change their passwords periodically and require them to achieve a minimum level of password complexity

5.2.3. Disks are encrypted using AES 256 technology.

5.2.4. Connectivity between TCR offices and TCR's hosting provider is protected using VPN technology

5.2.5. File transmissions use password protection features within Microsoft Office or Adobe Acrobat, for example, with passwords provided separately

5.2.6. From the portal, all access from the users is across TLS 1.0, 1.1, 1.2 (https), we have a A+ rating on https://www.ssllabs.com/ssltest/analyze.html?d=www.thecashroomportal.co.uk&hideResults=on

5.2.7. Always ensure that any device is not set up to automatically remember login details and passwords. The option to remember login information on web browsers must not be used.

## 6. Backup policy

This policy is designed to protect the company's data and ensure that it can be recovered in the event of equipment failure, intentional/accidental deletion or destruction due to fire, flood or any other such disaster. It is not the intention of this policy to ensure quick recovery of ad-hoc files that may have been deleted in error or have been updated incorrectly by the user. The restoring of such files may only be considered if they are required to fulfil a legal, contractual or regulatory obligation or a pressing business need.

Should computer systems become infected with malicious code (such as ransomware that encrypts data and requires payment to the criminal in order for the data to be unlocked) or a severe incident such as fire or flood, then restoring from a successful backup is the only way that the company could continue to do business.

### 6.1. Domain Controller/File Server

6.1.1. File level backup

Blowfish Technology Backup is backing up nightly the following folders on the file server:

Accounts, Q:Drive, Payroll, PortalShare, Scans

6.1.2. VM Level Backup

A Virtual Machine level image backup is taken monthly

### 6.2. Terminal Server

6.2.1. File level backup

Blowfish Technology Backup is backing up nightly the following folders on the TS server:

Accounts, SageBackups, Users

6.2.2. VM Level Backup

A Virtual Machine level image backup is taken nightly

### 6.3. Leo SQL Server

6.3.1. VM Level Backup

A Virtual Machine level image backup is taken nightly

### 6.4. Portal Virtual Machines

6.4.1. VM Level Backup

A Virtual Machine level image backup is taken nightly

### 6.5. Portal databases

There are a number of databases held across 2 systems, MySql and MongoDB.

A script which runs nightly on the database servers and "dumps" the database to a file on the server, this file is then compressed and encrypted using a GPG Encryption tool.

This compressed and encrypted file is then uploaded to an S3 bucket on Amazon, which is to an account which TCR owns.

### 6.6. Cloud Services

Staff are only allowed to open accounts on Dropbox, OneDrive, Google Drive and other such cloud services with the express permission of the Operations department.

Though these services offer the ability to store files off-site for safe keeping, it may be possible that the company is breaking contractual or regulatory obligations by storing information on these platforms.

### 6.7. Workstations, laptops, tablets and mobile devices

Information stored on the internal drives of company owned workstations and laptops are not backed up by default.

Workstation users must save all work to the central server (Q drive) unless authorised to save locally.

Laptop users, whilst in the office, shall save all files to the Q drive. Any work done off-site shall be moved (not copied) to the Q drive once back in the office.

## 7. Mobile and remote working policy

### 7.1. Background

When staff are required to work from remote locations, they shall ensure that sensitive data is not put at risk. The purpose of this policy is to inform staff about their own and the company's responsibilities regarding remote working and the use of mobile computer equipment or data storage devices outside company premises. Wherever staff are working, they must adhere to the same level of data protection as would be expected on company premises.

Mobile computer equipment is defined as: any device that can store and process information electronically. This includes laptop computers as well as smaller handheld devices such as smart phones, USB devices and memory cards.

7.1.1. If computer equipment is removed from the company's premises for any length of time, it must be stored securely.

7.1.2. Such equipment should never be left unattended in a staff member's car, on public transport or in the vicinity of anything related to commuting.

7.1.3. Non-members of staff or unauthorised persons must not be given the use of company-owned computer equipment or storage devices.

7.1.4. Always ensure that any device used in remote or home working is not set up to automatically remember login details and passwords. The option to remember login information on web browsers must not be used.

7.1.5. If using home computers, do so in line with the company's "Bring Your Own Device Policy".

7.1.6. Log out of systems if computers are left unattended (computers must be protected by passwords in line with the company's "Password Policy").

7.1.7. Staff making use of any third party equipment to access sensitive data must do so in accordance with the company's "Public Wi-Fi Policy".

7.1.8. Any company-owned computer equipment must be used in line with the company's "BYOD Policy".

7.1.9. If using home PCs and personal mobile devices, with express permission from the Operations team, they must be regularly backed up in line with the company's "Backup Policy". Staff must make regular audits of what is stored on these devices.

When discussing business in-person or on the phone, ensure that no sensitive information can be heard or seen by a third party.

7.1.10. Paper documents containing sensitive data must be securely locked away when not in use. Any such documents that are disposed of must be destroyed in line with the company's "Disposal and Destruction Policy".

7.1.11. Rules on the use of personally owned devices for remote working or data storage are set out in the company's "Bring Your Own Device Policy".

7.1.12. Staff making use of any third party equipment to access sensitive data must do so in accordance with the company's "Public Wi-Fi Policy".

### 7.2. Ongoing Commitments

At all times, staff must take measures to secure sensitive data while working outside the business premises. This requires that staff:

7.2.1. Log out of systems if computers are left unattended (computers must be protected by passwords in line with the company's "Password Policy").

7.2.2. Ensure sensitive information is not on view to people nearby. For example, this could include notes stuck to computer screens, minutes of meetings, financial reports and other items deemed sensitive by the company.

7.2.3. When printing sensitive documents, always ensure that documents are immediately collected from printers, fax machines or photocopiers.

7.2.4. In no circumstances must personal computers be used for remote or home working without the relevant authorisation in line with the company's "Bring your Own Device (BYOD) Policy".

## 8. Public Wi-Fi policy

### 8.1. Background

The company encourages work-related internet and email use whilst not on company premises as long as the devices used to achieve this have been sanctioned by the company.

Using public Wi-Fi to conduct business, without the necessary safeguards, places our data at risk of theft.

Staff are encouraged to always choose the most secure connection - even if that means paying for access and then turning off the wireless network when it is not in use.

For Security reasons staff must:

8.1.1. Not follow prompts to update software whilst connected to a public network;

8.1.2. Never transmit any data that is deemed "Confidential" or "Restricted" unless a secured VPN tunnel has been established and the user has been trained in setting up such a connection;

8.1.3. Be wary that URLs in web browsers are actually pointing to the expected place in case a criminal has hijacked the Wireless Access Point and is forwarding traffic to their site;

8.1.4. Ensure the connection is encrypted wherever corporate data is transmitted (check that HTTPS:// appears in the URL bar/address bar of the browser) even if the data is not deemed confidential or restricted;

8.1.5. Ensure that no-one can see the information being typed if in a public space.

Devices used on public Wi-Fi that are not sanctioned by the company include home PCs or those computers found in internet cafes, hotels or libraries for example.

Though the company takes every effort to ensure that devices are adequately protected, it is the responsibility of the individual to ensure that, before connecting to the Wi-Fi network, the device has:

8.1.6. Up-to-date antivirus and antispyware software;

8.1.7. A firewall that is activated and configured to company requirements (i.e. the settings have not been changed) since the device was issued;

8.1.8. All software (including your web browser) is current with automatic updating;

8.1.9. File sharing is switched off.

## 9. BYOD policy

### 9.1. Background

Though it is convenient to use personal devices such as smart phones, tablets and handheld or laptop computers for business purposes, there is no business reason for any member of staff to use their own device for business matters.

The company prefers the use of company owned/managed assets to connect to the business network, for storing as well as transmitting work-related material. This is because there is an increased security risk to our information systems when non-company equipment is used to process information or is connected to our network. Such risks include the loss or theft of the device leading to unauthorised access to emails and/or other services and the threat of malware.

If there is a compelling business need for individuals to use their own equipment for work-related matters, then a case shall be put forward to the line manager who will make a request to Operations to issue the required company-owned device. If there is still a need to use personal devices for work matters then this shall only be done in accordance with the policy outlined below.

Members of staff using their own devices for company use may only do so with the approval of senior management and must have agreed to this policy in writing.

### 9.2. Security requirements

BYOD users shall:

9.2.1. Use their best efforts to physically secure the device against loss, theft or unauthorised use;

9.2.2. Install approved anti-virus software;

9.2.3. Protect the device with a pin number or password;

9.2.4. Keep the operating system and applications current with security patches (within 7 days of release);

9.2.5. Only install software authorised by the company. A list of applications is available;

9.2.6. Not alter the security settings of the device without the company's consent;

9.2.7. Not download or transfer any company data to the device;

9.2.8. Not use the device as a mobile hot-spot without the company's consent;

9.2.9. Not copy company data to external devices (USB, CD/DVD drives) unless the user is authorised to do so and uses methods that are described in the "Backup Policy".

BYOD users understand the following:

9.2.10. Devices may be inspected by IT staff at any time to ensure they meet minimum standards, approved versions of patches, applications and anti-virus software.

9.2.11. Company data may be wiped from the device at any time during employment and when the user leaves the company. Although every effort will be taken not to erase the individual's personal data, there is no guarantee that personal data may not be lost.

9.2.12. Devices may only be used if they are on an approved list. If the device is not on the list, then the user may apply via email to the IT department to attempt to get the device approved.

9.2.13. If access to our systems is granted, then it may be necessary for a member of the IT staff to install specialist software to allow connection [VPN /Terminal Service etc.].

9.2.14. The company may monitor, intercept, review and erase all content on the device that has been created for, or on behalf of the company. It is possible that personal data may accidently be included in this.

**9.3. Technical Support**

9.3.1. The company does not provide technical support for BYOD devices. The user is responsible for any repairs, maintenance or replacement costs and services.

9.3.2. No loan devices will be given by the company whilst BYOD devices are being repaired.

9.3.3. If there is an issue with connectivity, IT staff will treat this as any other low priority support ticket.

## 10. Disposal and destruction policy

All sensitive information must be removed using approved methods. This requirement includes all data stored in systems, temporary files or information contained digitally that may reside in photocopiers, printers, USB drives, workstations, laptops and mobile devices, or on storage media, including DVDs/CDs/Tape/USBs etc.

When no longer required, paper documents must be stored in the secure bins provided, until they are collected by TCR's chosen document disposal company.

Devices may only be reused within the organisation and may not be sold on, or otherwise used for noncompany matters, unless the information has been deleted securely and approved by Operations.

Depending upon the sensitivity of the information, the company may not allow devices to be re-used outside of the company.

# SCHEDULE 3: DATA PROTECTION

This Schedule sets out the detail of how the Cashroom complies with its obligations. It is divided into 8 parts.

1. **Use of Client Data.** This part describes the data we collect from clients and sets out our reason for processing, explains how we keep the data safe, how long we keep it for, and when we destroy or return that data.
2. **Use of Employee Data.** This part describes the data we collect from Employees and sets out our reason for processing, explains how we keep the data safe, how long we keep it for, and when we destroy or return that data.
3. **Use of Marketing Data.** This part describes the data we collect from contacts and potential clients, and sets out our reason for processing, explains how we keep the data safe, how long we keep it for, and when we destroy or return that data.
4. **Suppliers Data.** This part lists the Data Processors and Sub-processors we use.
5. **Data Protection Impact Assessments.** This part explains how and when we carry out Data Protection Impact Assessments.
6. **Data Subject Requests**. This part sets out how we deal with Data Subject Requests.
7. **Data Breach Management and Reporting.** This part explains our Breach Notification Policy and the management and reporting in data incidents.
8. **Data Protection Compliance Monitoring Policy.** This sets out our internal and external audit process.

## SCHEDULE 3: PART 1 – USE OF CLIENT DATA

Broadly we gather 2 types of data from our Clients; data about our client's clients, and data about our clients and their business. Table [1] sets out the data we gather about our client's clients, and Table [2] sets out the data we gather from our clients.

**Table 1**

Clients clients' personal data policies

**Table 2**

Clients' personal data policies

## SCHEDULE 3 PART 2 – USE OF EMPLOYEE DATA

Table 3 sets out the data we gather about our Employees, why we process it, how we keep it safe, for how long we retain it, and how we destroy it when the reason for processing expires.

**Table 3**

Employee personal data policies

## SCHEDULE 3: PART 3 – USE OF MARKETING DATA

Table 4 sets out the data we gather from our contacts and from potential clients, why we process it, how we keep it safe, and when we delete it.

**Table 4**

Marketing personal data policies

## SCHEDULE 3: PART 4 – SUPPLIERS DATA

During the course of our business we share data with a number of suppliers. We do so to allow us to provide a better service to our clients, and help us to fulfil our obligations to Employees.

The GDPR requires us to ensure that any supplier, who processes personal data on our instructions provides sufficient guarantees that the requirements of the GDPR will be met and the rights of data subjects protected. We are also under an obligation to advise Data Controllers, for whom we are Data Processors, of the suppliers who have access to personal data.

We have risk assessed all our suppliers into low, medium and high risk based on the impact a data breach would have. The “guarantees” obtained are greater depending on our risk assessment.

A list of the suppliers who have access to personal data provided by clients, the data they have access to, our risk assessment, and the guarantees they have provided can be requested via the DPAdmin (dataprotection@thecashroom.co.uk).

Also, a list of the suppliers who have access to our employees’ personal data, the data to which they have access, our risk assessment, and the guarantees they have provided can be requested via the DPAdmin.

## SCHEDULE 3: PART 5 – DATA PROTECTION IMPACT ASSESSMENTS

A Data Protection Impact Assessment is a process to help the Cashroom identify and minimise the data protection risk of a project.

We will carry out a DPIA when we

1. Use new technologies
2. Combine, compare or match data from multiple sources
3. Process personal data without providing a privacy notice directly to the individual

We will consider carrying out a DPIA when we are:

1. Evaluating or scoring
2. Automatic decision making with significant effects
3. Processing sensitive data or data of a highly personal nature
4. Processing data on a large scale
5. When using Innovative technologies or organisational solutions
6. In any major project involving the use of personal data
7. Where there is a change to the nature, scope, contexts and purpose of our processing

If we decide not to use a DPIA we will document our reasons

A DPIA will

1. Describe the nature scope context and purpose of the processing
2. Assess necessity, proportionality and compliance measures
3. Identify and assess risks to individuals; and
4. Identify any additional measures to mitigate those risks.

If we complete a DPIA that identifies a high risk, and we cannot take any measures to reduce that risk, we will consult the ICO, and will not carry out the processing until we have done so.

We have trained our staff to recognise when a DPIA is necessary.

Primary responsibility for carrying out a DPIA rests with the project lead and will be overseen by our Data Protection Administrator.

## SCHEDULE 3: PART 6 – DATA SUBJECT REQUESTS

The Cashroom respects the following rights of Data Subjects

1. The Right of Access
2. The Right to Rectification
3. The Right to Erasure
4. The Right to Restrict Processing
5. The Right to Data Portability
6. The Right to Object

The Cashroom does not use personal data to make automated decisions or complete individual profiling.

This Part sets out the procedures in place to deal with requests from Data Subjects as regards these rights.

### 1. The Right of Access

Data Subjects have the right to access their personal data. That right allows individuals to be aware of and verify the lawfulness of the processing.

ALL DATA ACCESS REQUESTS SHOULD BE REFERRED TO THE DATA PROTECTION ADMINISTRATOR (the DPAdmin)

An access request can be made verbally or in writing. There is no “official” format. All employees who deal with clients must be aware that any request to access data should be treated as a formal access request, and referred to the Data Protection Administrator.

Data Subjects have the right to obtain

1.1. Confirmation that their data is being processed

1.2. Access to their personal data; and

1.3. The information that should be provided in a privacy notice.

The Cashroom will provide a copy of the data free of charge, within one month of receipt. If the requests are complex or numerous we will advise the Data Subject that we will provide them the information within 2 months, and explain why.

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, we will charge a reasonable fee for providing the information, or may refuse to provide the information. If we do so, we will explain why, and advise the Data Subject of their right to complain and to a judicial remedy, within one month.

We will provide the information only after confirming the Data Subjects identify. We will require photo ID (e.g. passport) and confirmation of their current address. If the request is made electronically we will supply the information in a commonly used electronic format.

### 2. Right to Rectification

Data Subjects have the right to have inaccurate personal data rectified.

ALL RECTIFICATION REQUESTS SHOULD BE REFERRED TO THE DATA PROTECTION ADMINISTRATOR

A rectification request can be made verbally or in writing. There is no “official” format. All employees who deal with clients must be aware that any challenge to the accuracy of data, should be treated as a formal rectification request, and referred to the Data Protection Administrator.

On reception of a rectification request we will take reasonable steps to assess the accuracy of the data we hold. While we are considering the accuracy of the data we will restrict the processing of that data. It is the role of the DPAdmin to investigate the request and present their finding to Operations Director who will decide whether to rectify the data.

If the Operations Director decides not to rectify the data they will advise the Data Subject that we believe the data to be accurate, and explain that we will not amend the data. We will advise them of their rights to complain to ICO, and their rights to seek to enforce their rights through a judicial remedy. We will place a note with the data that the Data Subject challenges the accuracy of that data.

The Cashroom will deal with a rectification request within one month of receipt. If the requests are complex or numerous we will advise the Data Subject that we will deal with the request within 2 months, and explain why.

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, we will charge a reasonable fee for dealing with the request, or may refuse to deal with the request. If we do so, we will explain why, and advise the Data Subject of their right to complain and to a judicial remedy.

We will deal with the request only after confirming the Data Subjects identity. We will require photo ID (e.g. passport) and confirmation of their current address.

If we amend the data we will advise any Data Processors to whom we have provided the data of the amendment.

### 3. Right to Erasure

Data Subjects have the right to have their personal data erased in the following circumstances

3.1. The Personal Data is no longer necessary or the purpose it was originally collected for has expired

3.2. If consent was the lawful basis for processing, they have withdrawn their consent

3.3. If legitimate interest was the basis for processing, the individual objects and there is no overriding legitimate interest to continuing to process

3.4. The purpose of processing is direct marketing and the individual objects to that processing

3.5. We have processed the data unlawfully, or;

3.6. We must do so to comply with a legal obligation.

The Right to Erasure does not apply if processing is necessary for one of the following reasons

3.7. To comply with a legal obligation

3.8. For statistical purposes, where erasure is likely to render impossible or seriously impair the achievement of that processing, or;

3.9. For the establishment, exercise or defence of legal claims.

An erasure request can be made verbally or in writing. There is no “official” format. All employees who deal with clients must be aware that any request to delete data, should be treated at a formal erasure request, and referred to the DPAdmin.

On reception of an erasure request we will restrict the processing of that data. It is the role of the DPAdmin to investigate the request and present findings to the Operations Director who will decide whether to erase the data.

If the Operations Director decides not to erase the data they will advise the Data Subject, and explain that we will not erase the data, and why. We will advise them of their rights to complain to ICO, and their rights to seek to enforce their rights through a judicial remedy.

The Cashroom will deal with an erasure request within one month of receipt. If the request is complex or numerous we will advise the Data Subject that we will deal with the request within 2 months, and explain why.

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, we will charge a reasonable fee for dealing with the request, or may refuse to deal with the request. If we do so, we will explain why, and advise the Data Subject of their right to complain and to a judicial remedy.

We will deal with the request only after confirming the Data Subjects identify. We will require photo ID (e.g. passport) and confirmation of their current address.

If we erase the data we will advise any Data Processors to whom we have provided the data of the erasure, and request that they do the same.

## 4. Right to Restrict Processing

Data Subjects have the right to restrict the processing of their personal data in the following circumstances

4.1. Where the Data Subject contests the accuracy of the data and you are verifying its accuracy

4.2. The data has been unlawfully processed and the Data Subject opposes erasure and request restriction instead

4.3. You no longer need the persona data but the individual needs to keep it in order to establish, exercise or defend a legal claim.

4.4. The individual has objected to you processing their data under Article 21(1) and we are considering whether our legitimate grounds override those of the individual.

A restriction request can be made verbally or in writing. There is no “official” format. All employees who deal with clients must be aware that any request to restrict data, should be treated at a formal restriction request, and referred to the DPAdmin.

It is the role of the DPAdmin to investigate the request and present finding to the Operations Director who will decide whether to restrict the data.

If the Operations Director decides not to restrict the data they will advise the Data Subject, and explain that we will not restrict the data, and why. We will advise them of their rights to complain to ICO, and their rights to seek to enforce their rights through a judicial remedy.

The Cashroom will deal with a restriction request within one month of receipt. If the request is complex or numerous we will advise the Data Subject that we will deal with the request within 2 months, and explain why.

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, we will charge a reasonable fee for dealing with the request, or may refuse to deal with the request. If we do so, we will explain why, and advise the Data Subject of their right to complain and to a judicial remedy.

We will deal with the request only after confirming the Data Subjects identify. We will require photo ID (e.g. passport) and confirmation of their current address.

If we restrict the data we will advise any Data Processors to whom we have provided the data of the restriction and request that they do the same.

## 5. The Right to Data Portability

The right to data portability allows individuals to obtain and rescue their personal data for their own purposes across different services when

5.1. The individual provides personal data to a Data Controller

5.2. Where the processing is based on the individuals consent or for the performance of a contract, and;

5.3. When processing is carried out by automated means.

In these circumstances the Cashroom will provide the personal data in a structure commonly used and machine readable form, within 1 month of the request.

**6. Right to Object**

Individuals have the right to object to

6.1. Processing on the basis of the Cashroom's legitimate interests

6.2. Direct marketing, and;

6.3. Processing for the gathering of statistics

If a Data Subject objects to processing on the basis of the Cashroom's legitimate interests we will stop processing unless

6.4. We have compelling legitimate grounds for the processing which override the interests rights and freedoms of the individual, or;

6.5. The processing is for the establishment, exercise or defence of legal claims.

If the Data Subject objects to processing for the purposes of Direct Marketing we will stop processing Personal Data immediately.

If the Data Subject objects to processing for statistical purposes we will stop processing Personal Data immediately.

## SCHEDULE 3: PART 7 – DATA BREACH MANAGEMENT AND REPORTING

The Cashroom is under an obligation to report Personal Data Breaches.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

ALL CASHROOM EMPLOYEES ARE RESPONSIBLE FOR REPORTING DATA BREACHES TO THE DATA PROTECTION ADMINISTRATOR (DPAdmin - dataprotection@thecashroom.co.uk).

The DPAdmin will report the breach immediately to the Operations Director and initiate an investigation of the breach. If the DPAdmin and the Operations Director believe that a data breach has occurred the following process(es) will be implemented.

**1. Data Breaches Register**

The Cashroom maintains a Data Breaches Register to record all data breaches.

**2. Reporting a Data Breach to Data Controllers**

Where we are a Data Processor, for example, where we process our client's clients data, we must report the data breach to the Data Controller (here, our client) immediately. It is then for the Data Controller to decide whether to report the breach to ICO, or to the Data Subjects.

**3. Reporting a Data Breach to ICO**

Where we are the Data Controller, we are under an obligation to report a data breach to ICO where the data breach is likely to result in a risk of adversely affecting individuals' rights and freedoms. This is a decision for the Operations Director and they will make that decision based on all relevant factors.

Where a decision is made not to report a data breach to ICO, the reason for not reporting the breach is recorded in the Data Breaches Register.

A data breach must be reported within 72 hours of becoming aware of the breach. The report must contain

3.1. A description of the nature of the Personal Data breach including the individuals concerned

3.2. The name and details of the Data Protection Administrator

3.3. A description of the key consequences of the personal data breach

3.4. A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including where appropriate the measures taken to mitigate any possible adverse effects.

### 4. Reporting a Data Breach to Individuals

Where we are the Data Controller, we are under an obligation to report a data breach directly to Data Subjects where the data breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms. This is a decision for the Operations Director and they will make that decision based on all relevant factors.

The main reason for informing individuals as quickly as possible is so they can take steps to protect themselves from the effects of a breach.

Where a decision is made not to report a data breach to individuals, the reason for not reporting the breach is recorded in the Data Breaches Register.

A data breach must be reported without undue delay. The report must contain

4.1. A description of the nature of the personal data breach

4.2. The name and details of the Data Protection Administrator

4.3. A description of the key consequences of the personal data breach

4.4. A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including where appropriate the measures taken to mitigate any possible adverse effects.

## SCHEDULE 3: PART 8 – DATA PROTECTION COMPLIANCE MONITORING

To ensure compliance with our DPP, the Cashroom will train its staff in their obligations and monitor compliance.

### 1. Staff Training

All new staff will receive training on their obligations under the GDPR, and under our DPP within 1 month of starting with the Cashroom. In addition all staff will receive yearly update training.

### 2. Internal Audit

The Data Protection Administrator is responsible for carrying out an internal compliance audit with our DPP every 6 months.

The DPADMIN will report the outcome of that audit to the Board, along with any recommendations on changes and updates to the policy.

### 3. External Audit

Once a year our DPP is audited by an external auditor.