# General Data Security Policy

**10th July 2025**

**FCA number: 744359**

Clearway | Financial | Solutions

# Table of Contents



**Please read in conjunction with our 'Data Protection & Cookies Policy' 2025.**

## Purpose of Our Data Security Policy

The main purpose of this security policy is to inform staff and managers of their obligatory requirements for protecting technology and information assets. This policy specifies the mechanisms through which these requirements can be met. Another purpose is to provide a baseline from which to acquire, configure and audit our internal systems and processes for compliance with the policy.

This Policy may be read in conjunction with our Data Protection & Cookies Policy, Disaster Recovery Plan and Business Continuity Plan.

**What Needs Protecting?**

The key assets requiring protection through a security policy have been identified as:

1. Hardware: CPUs, boards, keyboards, terminals, workstations, personal computers, laptops, IPads, IPhones, printers, disk drives, communication lines, terminal servers, routers.

2. Software: source programs, object programs, utilities, diagnostic programs, operating systems, communication programs.

3. Data: during execution, stored on-line, archived off-line, backups, audit logs, databases, in transit over communication media.

4. People: users, administrators, hardware maintainers.

5. Documentation: on programs, hardware, systems, local administrative procedures.

6. Supplies: paper, forms, ribbons, magnetic media.

For convenience we have broken these assets down into specific business areas which we need to protect – Physical Security, IT Security (see also Data Protection & Cookies Policy 2025), and Intellectual Property.

## Physical Security

These are the means by which we ensure that premises and documents are kept secure from unauthorised access.

**Protecting the Building**

The building (9a Barton Road) is protected from unauthorised access by:

1. An Intruder Alarm (front and rear access), which conforms to regulations.

   The system is checked and maintained every 12 months by the Diverse Security https://diversesecurity.com/

   Access to the address is only available to the staff/introducers listed in Appendix 4 of this policy.

**Protecting Documents in the Office**

Documents are protected from unauthorised access by:

1. Keeping minimum paper records/documents in the office. We prefer to scan all paperwork and shred any confidential paperwork immediately. We operate a paperless office policy.

2. All confidential waste paperwork is shredded. All other non confidential waste is shredded on the premises and is sent for recycling.

3. All client documents are scanned into their computer file and the True Potential back-office system.

4. For security we store all client files on two types of media: True Potential back-office system and Windows cloud.

If any IT administration processes such as back up of data, support of the various IT systems and data storage are outsourced the specific procedures will be followed and due diligence on the firms concerned carried out.

The staff of the outsourced IT provider (Convene IT), whose staff can access client data are to be also subject to our due diligence procedure.

Our procedures will include:

1. Understand the third party's data security procedures – see separate document (Convene Security Standards 1.1).

2. Carry out appropriate due diligence on those third parties, including their security arrangements and staff recruitment policies.

3. Consider whether they should allow third parties unsupervised access to the office or records.

## IT Security

These are the means by which we ensure that any electronically stored information is kept secure from unauthorised access.

**Protecting Infrastructure and Hardware**

Servers, personal computers and laptops are protected by external attack from unauthorised access, viruses and Trojan Horses by:

1. Complex password policy is enforced on all servers, personal computers and Laptops. All passwords must be at least eight characters long and include one capital letter, one number and one special character. Users are then encouraged to change their own password regularly .

2. All staff are provided with an individual UNIPASS certificate. This is administered and controlled by the Data Protection Officer, Mr Mike Old.

3. There is firewall protection in place, a boundary Firewall and software firewall managed by Convene IT

   All workstations are installed with WINDOWS DEFENDER, which helps stop, remove and prevent the spreading of viruses, worms or trojans.

4. Data encryption is by way of Unipass or Securemail in Microsoft Outlook (Azure Information Protection Premium P1 licenced). Emails containing sensitive data are sent to clients and third parties by this method. Given the number of staff employed by Clearway Financial Solutions, our internal computer data is not encrypted, as it is deemed the risk is too small to warrant the cost of encrypting all internal data within the firm.

5. All devices (desktop & laptops) are encrypted via BITLOCKER.

6. All incoming emails are scanned for viruses and other threats by Microsoft 365 before they are delivered onto the network. We also have 'Convene Cyber' screening emails – see 'monthly' reports.

7. All incoming emails are filtered for SPAM and quarantined for checking by Convene Cyber/Microsoft 365 before they are delivered onto the network.

8. Remote access to workstations is via RMM software managed by Convene IT.

9. Wireless network is secured via WPA.

10. Use of personal and web-based email are prohibited by the network software controls.

11. The use of USB memory sticks are strictly controlled so as to prevent the introduction of viruses and loss of data.

12. Staff are discouraged from opening emails or attachments from unknown sources as these could be a source of Phishing attacks. Quarterly Security Awareness Tests and Training are sent to limit the organisation's exposure to cyber fraud and attacks. We have quarterly testing (provided by Convene Cyber) to embrace these risks and know what to look out for.
    ID Agent - Security Awareness Training - Get a Demo | ID Agent

13. Client information is held online, via True Potential LLP, and is securely protected via 128 bit encryption and requires a User Name, Password and random Passphrase to enter.

14. Network and individual computer administration rights are controlled through the System Administrators, Mike Old, Trudi Old and Matthew McLellan Grant and for monitoring purposes, Convene IT.

15. Staff may not undertake work on their own personal computer.

**Disposal of Hardware**

Consideration is given to the disposal of computers, laptops, memory sticks, disks etc.

1. If a third party is used for the disposal of data, the firm will satisfy itself with their security and staff vetting arrangements.

2. Disposal of a computer - the hard drive will be wiped with specialist software or removed and destroyed sufficiently so that information cannot be accessed by an authorised person.

## Protecting Intellectual Property

These are the additional means by which we ensure that our intellectual property, and the goodwill of the business, is kept secure from unauthorised access.

**Staff**

Staff are made aware of their obligations through their:

1. Employment / Self Employed contract

2. Induction process which covers this security policy

3. Regular training and testing on data security/cyber scams/attacks (Convene Cyber)

4. Updates to changes on security policy

5. Annual test on GDPR (Paradigm Compliance)

6. Annual AML, Financial Crime Training and testing (Paradigm Compliance)

7. Annual Cyber Security training (Paradigm Compliance)

Use of all company equipment is governed by the Staff procedures which state that:

1. All company equipment is logged against staff member.

2. Laptops must be locked away and not left in insecure locations [e.g. cars overnight].

3. Files of any kind must not be taken home.

4. Staff may not undertake work on their personal computers.

5. Staff may not email work to personal email accounts.

**Staff Leavers**

The business is protected from employed and self-employed staff who leave the firm, as follows:

1. All property including Office keys and entry keys must be returned to the company on leaving.
2. Staff can be placed on 'gardening leave' on resignation.
3. Restrictive covenants are in place to prevent solicitation of clients after leaving.
4. Staff Contracts makes explicit reference to Confidential Information and ownership of client data.

**Access Rights**

Access rights to information on the network and emails are controlled through an Access Right Policy. Full detail is contained within the Policy but this ensures that:

1. Access is granted to data only where required and where approved by Mike Old.
2. Temporary access to data must also be time bound, and privileges revoked after that date or an extension expressly granted by Mike Old.
3. Network administration is subject to annual Credit Check and Criminal Records Bureau check on appointment, in addition to full referencing etc.
4. All staff who access client/sensitive information are subject to an annual vetting process (this could include Credit Checks and/or Criminal Records Bureau checks).
5. A register is maintained listing what access rights have been given and to which staff. This is maintained and updated by Mike Old.

## Requests for and Exchange of Information

**Telephone**

All inbound calls from clients, for which staff do not recognise their voice, are subject to verification of their date of birth, postcode and knowledge over 1+ policies held (as recommended by us). Or for the following:

1. Change to any contact details.
2. Request for any copy correspondence previously issued by post.
3. Request for any values or policy information previously issued by post.
4. Any other suspicious requests or requests for information which might reasonably be used for fraud.
5. Calls from a client's close family are verified by ringing the client to confirm authentication of the person and client's permission to speak with them on non-personal details.

**Email**

All email requests from clients for the following are subject to verification by contacting the client by telephone and verifying the request using SecureMail, if active with that client, for the following:

1. Change to any contact details.
2. Request for any copy correspondence previously issued by post.
3. Request for any values or policy information previously issued by post.
4. Any other suspicious requests or requests for information which might reasonably be used for fraud.

All email correspondence sent back to the client containing policy details or any other personal information, must be sent using the following methods:

1. Posted to secure message service available at [True Potential and Cashcalc Client Portal].
2. Sent using our email encryption software SecureMail or via Windows Office 'One Drive'.
3. Have a password protecting any documents/attachments.
4. Sent via conventional post to address on file.

**Letter**

All requests by letter from clients for the following are subject to verification by contacting the client by telephone and verifying the request for the following:

1. Change to any contact details.
2. Request for any copy correspondence previously issued by post.

3. Request for any values or policy information previously issued by post.

4. Any other suspicious requests or requests for information which might reasonably be used for fraud.

5. All correspondence sent back to the client containing original client documents, must be sent using recorded delivery or hand delivered.

**Request for Information Under the Data Protection Act**

Any individual requesting information held on them under the Data Protection Act has a right to such information, subject to certain limitations. All such requests should be forwarded to Mike Old, who is responsible for the processing of such requests. Under no circumstances should staff provide this information without reference to Mike Old.

## Security Violations/Data Compromise Reporting Policy

All staff are under an obligation to report any incident which they may feel violate the security of the company by informing Mike Old immediately. If he is not in the office, he must be telephoned or texted immediately. All violations are to be recorded in the Security Violations Register.

Equally all staff is aware of the need to report any data compromise incidents. These can include:

1. Loss of laptop
2. Loss of client data either in paper form or electronic
3. Loss of memory sticks/disks/USB pens etc
4. Unauthorised persons in back-office area where data stored
5. Client information passed onto unauthorised third party
6. Any unusual activity encountered while working on an office computer or back-office application.

All incidents should be reported immediately to Mike Old, these will be investigated and if a compromise has been found, it is to be a entered up on a Data Compromise Register. The firm's policy for a serious breach will be in the first instance report this to the police and then to the client concerned, detailing what actions will be taken.

## Audits

Compliance with this policy is audited on an annual basis by Mike Old. The results are detailed in the Security Audit Log.

## Important Contact Information

Third Party IT Provider

Convene IT
Unit 1a
Sandham Street
Chorley
Lancs
PR6 0RA

Tel: 01257 272261

Email: contact@conveneit.co.uk
Email: support@conveneit.co.uk

Web: www.conveneit.co.uk

Website Administrators

IFA Portals
Portal House
65 Dale Street
Rochdale
Lancashire
OL16 3NJ

Tel: 01706 351812

Email: info@adviserportals.co.uk
Web: www.adviserportals.co.uk

## Back Office Providers

**True Potential**
Newburn House
Gateway West
Newcastle upon Tyne
NE15 8NX

Tel: 0191 242 4876
adviserservices@tpllp.com

## Third Party Cyber Partner

Convene Cyber
Unit H2/H3
Cassidy Court
Salford
M50 2QW

Tel: 0343 4149900

Email: hello@convenecyber.com

Web: www.convenecyber.com

Appendix 1

Current key holders are:

Mike Old
Trudi Old
Matthew McLellan Grant
Andrew Rourke
Caroline Whelan