The Wisdom Council

Business Systems & Risk Controls Policy

Last updated: December 2025

Policy Contents

Alison Malton	December 2025
Reviewed By	**Date last reviewed**

1. Introduction to our Business Systems & Risk Controls Policy

This document is designed to be a centralised policy for The Wisdom Council. Our practices and ways of working relating to IT, other business systems and risk are addressed within this document. It is reviewed on an annual basis and approved by senior management.

---

2. Data Protection Policy

The Wisdom Council (TWC) takes Information Security seriously and is committed to ensuring that personal and confidential data is secure from risk of loss, theft or corruption.

This policy refers to the collection, storage and handling of personal and confidential data:

- Personal data is any information relating to an identifiable person who can be directly, or indirectly identified in particular by reference to an identifier.
- Confidential data is any information that is not intended for public dissemination.

Responsibilities:

- Everyone who works for The Wisdom Council (TWC) has some responsibility for ensuring personal and confidential data is collected, stored and handled appropriately. Each individual that handles data must ensure that it is handled and processed in line with this policy and data protection principles.

- The data protection lead for The Wisdom Council will be responsible for informing colleagues (existing and new) of their data protection responsibilities and ensuring compliance within the organisation.

- The Wisdom Council will provide training to all employees to help them understand their responsibilities when handling data.

Employee handling of data:

All employees confirm that they will:

- Not make any use of the data or allow any use of the data except for the purpose agreed with TWC Partners.
- Only access personal and confidential when required to do so for their work.
- Hold data in confidence and will not disclose or allow the disclosure of any part of the data to a third party without verifying the identity of that third party and where they are an approved subcontractor and an appropriate contract is in place.
- Endeavour to safeguard the data from unauthorised or unlawful processing or accidental loss, destruction or damage of the data.
- Ensure that they understand their responsibilities under the General Data Protection Regulation (GDPR) where TWC is acting as a controller or processor of data.

- Employees should request help from their line manager if they are unsure about any aspect of this policy or their responsibility when it comes to storing, handling and disposing of data.

Employment policies:

The following procedures are applied:

- New employees, contractors and consultants are verified prior to commencement of employment and reasonable steps are taken during the recruitment processes to ensure the reliability of all new employees, including but not limited to verifying passports, carrying out background checks and verifying provided references.
- All staff are aware of the key principles and their responsibilities under our Information Security Policy and the General Data Protection Regulation (GDPR).
- A financial crime and compliance training should be done as part of the employee onboarding process (with refresh on ad-hoc basis). The aim is to educate employees and raise awareness around these threats. The training process covers not only fraud, anti-bribery and conflicts of interest as per our standards of business conduct, but also critical aspects of financial risks and threats in the context of our business practice, including helping employees identify instances where this can happen in practice, practical ways to handle said incidents and steps they need to take to prevent them from happening.
- All staff are required to enter into confidentiality undertakings as part of their employment terms.
- On joining, all staff are given a copy of the Information Security Policy and requested to confirm their understanding and agreement.
- Facilities and System access is restricted on termination of employment.

Physical security:

- Adequate protections are made against accidental lost through burglary, fire, or natural disaster.
- Physical access to the office (at 33 Cannon Street, City of London, EC4M 5SB) is controlled via a permanently manned reception (both during and outside office hours).
- The dedicated TWC offices are to be locked whenever left unattended.
- There is a controlled procedure for who has keys to the office which is restricted to employees.
- A clear desk policy is implemented.
- Any physical copies of confidential or personal data must be kept securely (in locked drawer or cabinet) where unauthorised individuals cannot access it.
- When no longer needed, any physical copies of confidential or personal data should shredded and disposed of securely.
- When no longer needed, any physical media (e.g. USB stick or CD) should be destroyed professionally via Inhouse IT.

IT security:

- **Infrastructure**
  - All data is stored within the Microsoft for Business Office 365 environment.
  - Personal and confidential data should only be stored and accessed on TWC computers - these are equipped with approved security software (including centralised anti-virus, Trend Micro) and BitLocker.
  - All accounts have dual-factor authentication enabled.
  - Reliance is made on the security protocols and procedures of Microsoft.
  - Access to the Microsoft environment is password controlled, and each user has a unique username and password.
  - Access is allocated on a Least Privilege basis and is role based, with new access requests authorised by a Director.
  - The Microsoft environment provides encryption of emails.

- **Data:**
  TWC classify data and the related security control into four categories:
  - Green = Public
  - Black = Internal or Council/Client Specific
  - Orange = Restricted
  - Red = Highly Confidential

  All confidential and personal data is classified as Orange or by exception Red.

  On SharePoint within the Microsoft environment, libraries are established which will have an assigned security level. Groups will be assigned access to them accordingly. Access is controlled via a SharePoint administrator with authorisation from a Director.

  - Green = Public.
    - TWC Employees Full Access & External Groups Read Only Access
  - Black = Internal or Council/Client Specific
    - TWC Employees Full
  - Orange = Restricted
    - TWC Employees Full/Read Only or Individual Access determined by folder content
  - Red = Highly Confidential
    - Individual employees with view only access on a need-only basis
    - Individual employees with edit access on a need-only basis

Third parties

- TWC may, subject to any specific terms agreed with a TWC client, use a sub-contractor to deliver part of the services.
- TWC will undertake due diligence on that contractor based on a risk assessment of the nature of the data which will be disclosed.
- Any disclosure of data to a sub-contractor is subject to a written contract which must be approved by a Director.
- Relevant due diligence must ensure evidence of a plan of the technical and organisational means the third party has adopted to prevent unauthorised or unlawful processing of or accidental loss of or destruction of the data.
- The contract must contain data security obligations which are no less onerous than those set out in the TWC Information Security Policy.

Governance

- Information Security is the responsibility of the Board of Directors which approves this Information Security Policy.
- At least annually the policy will be reviewed, and all employees will be reminded of their obligations under the policy.

As well as the above processes, the following guidelines must be followed with regards to specific aspects of collecting, storing and handling personally identifiable data:

Data storage:

- When storing confidential or personal data electronically, strong passwords must be used and should never be shared other than with designated parties, and only through a different media than the data was shared via.
- A 'strong password' is a password which meets the following minimum standards:
    a. at least twelve (12) alpha-numeric characters;
    b. not be trivial, based on public information, guessable, etc.;
    c. to be changed upon first use and thereafter within a reasonable period of time;
    d. not recycling or reusing of ten (10) previous passwords;
    e. initial passwords and password resets to be random; and
    f. passwords for Privileged Access to be subjected to stronger control requirements commensurate with the nature, sensitivity and value of the system and data they protect and related risk exposures.
- Passwords must never be written down and stored on paper and passwords stored within systems are to be securely encrypted.
- Initial or reset passwords to be communicated using a secure manner; unprotected (clear text) electronic mail message to be allowed only when sent with no other identifiable information.
- Passwords to individual employee accounts and computers must never be shared.
- If there is a belief that a password has been compromised, it must be changed immediately.
- All data files to be titled clearly in pre-agreed format (e.g. Client Name, Project Number and Name, Respondent Data).
- When new versions of data are created – consider whether all old versions need to be kept. If not, then delete.
- If confidential or personal data is stored on a removable device (e.g. USB stick/audio recorder/CD) these should be kept locked away when not in use and data should be removed as soon as possible.
- Confidential or personal data is to be removed from portable devices as soon as possible (e.g. audio recordings should be transferred onto a computer and deleted from the device within 24 hours)
- Where possible avoid storing confidential or personal data on individual TWC office computers, instead use SharePoint as key storage point.
- Data need only be stored and accessed on TWC office computers when that individual needs to edit it. As soon as they have done so, it should be uploaded to SharePoint, and deleted from the individual's computer files.
- Confidential or personal data should never be saved or downloaded directly to non-TWC computers, laptops, tablets or mobiles (including home computers and laptops used by TWC staff who may work remotely).
- Delete desktop 'Downloads' folder once a week to ensure no data is being inadvertently stored.

Data use:

- Employees should ensure the screens of their computers are always locked when left unattended.
- Data should not be shared informally. When access to confidential or personal data is required, employees can request to be given the formal access channels.
- Personal data, other than basic contact details should not be shared via email.
- Only send confidential data to external sources via a SFTP site or a password protected document.
- Share passwords verbally in person or over the phone, or via text message.
- Any passwords that are recorded should be stored securely in KeePass or similar password manager software.
- Data is to be held in as few places as necessary. Employees should not create any unnecessary additional data sets.
- Data should be updated as inaccuracies are discovered – for instance, if a respondent can no longer be accessed on their stored number/email address, it should be removed from the database.
- Data should be regularly reviewed and updated – if no longer required it should be deleted or disposed of in line with this policy document.

Data breaches:

- In the event of a data breach, the individual must let their line manager know as soon as the breach has been discovered. It is then the responsibility of the individual's line manager to inform the data protection lead who, when appropriate to do so, will inform the Board.
- If the breach is likely to result in a high risk to the rights and freedoms of individuals, TWC must inform those concerned (directly if The Wise Society, or where the data is ultimately owned by a client or supplier, we will inform them and help them determine how to let the individuals concerned know).
- If TWC suffers any data breaches that are likely to result in a risk to the rights and freedoms of persons involved, it is the data protection lead's responsibility to inform the Information Commissioner's Office (ICO) of the breach within 72 hours. This contact should outline:
    - a description of the nature of the personal data breach including, where possible:
        - the categories and approximate number of individuals concerned; and
        - the categories and approximate number of personal data records concerned;
    - the name and contact details of the data protection lead or other contact point where more information can be obtained;
    - a description of the likely consequences of the personal data breach; and
    - 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.
- All breaches, their effects and remedial action taken must be recorded internally, regardless of whether they are reported to the ICO.
- For all incidences it must be determined whether it was the result of human error or a systemic issue, and how a recurrence can be prevented.

Data retention policy:

- Confidential or identifiable personal data used for research purposes (i.e. where an individual can be identified by the information provided; e.g. sample lists, video/audio recordings, transcripts that include personally identifiable information, paper questionnaires, electronic data were named personal information and/or identifying information is captured) will be retained for as long as required.
- Personal Data relating to a member of one of our communities will be kept for as long as that individual is a member of that community and for 12 months after they request to no longer be a member or the community is closed.

Personal Data Access requests:

All individuals whose data is held by the company are entitled to:

- Ask what information the company holds about them and why.
- Ask how their personal data is used.
- Be informed how to keep it up to date.

If an individual contacts The Wisdom Council requesting to be informed of the personal data the company holds on them, they must provide this within 30 days of receiving the request.

If an individual contacts The Wisdom Council requesting their personal data be removed/'forgotten' by the company, they must do so within 30 days of receiving the request.

Providing information:

For The Wise Society (TWS) members, The Wisdom Council aims to ensure that individuals are aware that their personal data is being processed and that they understand:

- How the data is being used;
- How to exercise their rights.

To this end, TWS members agree to a privacy statement in the Terms and Conditions signed on becoming a member which can be found at:
https://communities.thewisdomcouncil.com/a/the-wise-society-terms-conditions

For personal data provided by clients and external recruiters:

- TWC clients and suppliers who provide personal data of individuals must confirm that the data provided has been collected in compliance with General Data Protection Regulation (GDPR)
    - For individuals' data which is collected by clients and suppliers, they must confirm that active consent was given for their data to be collected and that individuals were made aware of how:
        - Their data is being processed
        - Their data is being used
        - To exercise their rights.
- TWC should only accept data that is required for the purpose of the research project that is being conducted. Any irrelevant data provided is to be returned and/or deleted from TWC's systems.

Other Communities and TWC Relationships

For our other communities such as the Family Wealth Forum, the HNW community and for our general relationship management purposes, we will inform clients of our data protection policies via a Privacy Statement which will be posted on our website and can be found at https://www.thewisdomcouncil.com/privacy-policy/

---

3. Employment Related Policies

3a. Pre-screening Policy

At The Wisdom Council (TWC) we want to provide a safe working environment for everyone and make sure that everyone we recruit has the required qualifications and experience. As a result, we use 'Reed Screening' to perform pre-employment checks.

Our Reed Screening covers each of the below:

a) ID Check

b) Right to work in the territory (United Kingdom)

c) Criminal Record Check

d) Public Media Check

e) Credit Check

f) Employment History Check

g) Education and Required Qualifications Check

h) Confirmation that there are no legal or regulatory restrictions on staff that provide the service

Reed Screening also covers the procedure to evaluate a candidate and document results of pre-employment screening. TWC will then cover the process to reject those who fail the pre-screening checks.

3b. Termination Policy

Termination of employment refers to discontinuation of an employee's contract. This may be due to company discretion or the employee's actions.

The termination can further be categorised as voluntary or involuntary.

Voluntary separation may include the following:

- Resignation
- Retirement
- Failure to report to work without notice or lawful cause

- Expiration of a fixed-term contract

In case of resignation, an official resignation letter must be submitted by the employee to the line manager. The letter must give notice consistent with the minimum notice requirement, to enable the company to make alternative arrangements. The letter must be copied and submitted to senior management. Prior to the individual leaving the company, they will be reminded of their continued obligations with regard to data security and confidentiality, asked to return or delete all confidential data they hold and to return any company devices and other assets.

Involuntary dismissal may include the following:

- Discharge for cause
- Discharge without cause

These will follow our processes as set out in the employment of contract and in accordance with all applicable employment legislation. Again, prior to leaving the individual will be reminded of their continue obligations with regard to data security and confidentiality.

---

4. IT Related Policies

4a. Asset Return Policy

This policy is produced to provide a clear instruction on the appropriate management and return of physical IT assets.

All IT assets purchased by The Wisdom Council are the property of Wisdom Global Limited and will be deployed and utilised in a way that is deemed most effective for addressing the company's needs and objectively demonstrates value for money.

All IT assets must be assigned to individual users who will be held responsible for their care and security at all times whether they are in use, storage or movement.

End users must always contact a supervisor if they need to move, reassign or return IT equipment. All IT assets that are no longer in use must be returned to the company for redeployment.

4b. Password & 2FA Policy

Passwords

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of The Wisdom Council's (TWC) entire corporate network. As such, all TWC employees (including contractors and vendors with access to TWC systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

This section of the policy establishes a standard for the creation of strong passwords, the protection of those passwords and the frequency of change.

- A ‘strong password’ is a password which meets the following minimum standards:
    g. at least twelve (12) alpha-numeric characters;
    h. not be trivial, based on public information, guessable, etc.;
    i. to be changed upon first use and thereafter within a reasonable period of time;
    j. not recycling or reusing of ten (10) previous passwords;
    k. initial passwords and password resets to be random; and
    l. passwords for Privileged Access to be subjected to stronger control requirements commensurate with the nature, sensitivity and value of the system and data they protect and related risk exposures.
- Passwords must never be written down and stored on paper and passwords stored within systems are to be securely encrypted.
- Initial or reset passwords to be communicated using a secure manner; unprotected (clear text) electronic mail message to be allowed only when sent with no other identifiable information.
- Passwords to individual employee accounts and computers must never be shared.
- If there is a belief that a password has been compromised, it must be changed immediately.

✅ **Example of a good ‘strong password**
Password: My$ummerWalks2023

Why this is a good password?

- Has 12 or more characters
- Includes uppercase, lowercase, numbers and a special character (`M`, ‘n’, `9`, `@`)
- Not based on a person’s name, birthday or company information
- Random and unique, not reused elsewhere
- Easy to remember, but hard to crack and uses a phrase-like structure

❌ Example of a bad or weak password
Password: Password123

Why this is a bad/weak password?

- Only 11 or less characters (fails minimum length)
- Based on a common and guessable word
- Used widely across the internet in password dumps
- No special characters
- Likely reused or recycled across multiple accounts

💡 Tip for users
Use a “passphrase” approach, combining 3-4 unrelated words with numbers or symbols (e.g. `Sunset!River9Journey`). This makes passwords both memorable and secure while meeting all security requirements.

<u>2FA</u>
This section of the policy establishes a standard for the use of two-factor authentication.

Two-factor authentication (2FA), sometimes referred to as two-step verification, is a security process that involves users providing two separate forms of authentication to verify their identity and obtain access to an account or other sensitive materials. All employees at The

Wisdom Council must have two-factor authentication set up on the following platforms:

- Microsoft Office 365
- HubSpot
- Xero
- Freshdesk
- Ex-Plor
- Recollective
- WordPress
- SiteGround
- Vimeo
- Ayda
- Forsta

4c. Policy on use of Cloud Services

This policy applies to all persons accessing and using 3rd party services capable of storing or transmitting protected or sensitive electronic data that are owned or leased by The Wisdom Council.

The purpose of this policy is to ensure that sensitive data is not inappropriately stored or shared using public cloud computing and/or file sharing services.

The following table outlines the data classification and proper handling of data.

Data Classification	Cloud Storage (inc. Office 365 & Ridgeon)	Local Storage
Sensitive Data - Any data that contains personally identifiable information concerning any individual	**Allowed** Provided appropriate account controls are in place	**Not Allowed**
Public Data - Any data that does not contain personally identifiable information that TWC is comfortable sharing	**Allowed** No special requirements	**Allowed** No special requirements

4d. Incident Management Policy

Incident management is the ability to react to security incidents in a controlled, pre-planned manner. Preparation and planning are key factors to successful information security management and all The Wisdom Council (TWC) systems rely on Incident Management Plans for safe and secure operations.

For the purposes of this policy, an incident is defined as any event or action which results in an actual and/or potential compromise of an IT asset or Information Asset (including personal data).

<u>Types of Incidents</u>

IT Security related incidents include (but are not limited to):

- Detection of malicious code (e.g. viruses and malware);
- Network attacks or Denial of Service (DOS) attacks;

- Unauthorised access to an IT system;
- Accidental loss of personal or other information assets;
- Deliberate release of personal or other information assets.

In the event of any of the incidents listed above, the individual must let their line manager know as soon as the incident has been discovered. It is then the responsibility of the individual's line manager to inform the data protection lead who, when appropriate to do so, will inform the Board.

The individual's line manager will be responsible for recording and escalating the incident with the relevant stakeholders including; senior management, the board, clients and 3rd party suppliers where applicable.

4e. Personal Mobile Device Management Policy

Where personal employee devices are permitted, access to organisational systems and data is controlled through Microsoft Intune mobile device management and conditional access policies. All devices must meet Cyber Essentials Plus–aligned security requirements before access to internal network or systems is granted.

Key controls include:

- **Device compliance enforcement:** Devices must have an active screen lock (PIN, password or biometric), encrypted storage and be running a supported and up-to-date operating system (i.e. the latest iOS for Android systems).
- **Conditional access:** Access to corporate services (e.g. email, collaboration tools such as MS Teams) is blocked or restricted if a device is non-compliant.
- **Data segregation:** Corporate data is logically separated from personal data using managed applications and policies to prevent unauthorised sharing, copying or storage.
- **Malware and threat protection:** Platform-native security controls are required (e.g. iOS/Android security features) and monitored via Intune.
- **Remote management and response:** The organisation can selectively wipe corporate data from a personal device if it is lost, stolen, compromised or when access is no longer required.
- **Monitoring and audit:** Device compliance status is continuously monitored to ensure ongoing adherence to security requirements.

These controls ensure that sensitive information remains protected while allowing limited use of personal devices in a controlled and auditable manner.

---

5. Business Continuity & Disaster Recovery Policy & Plan

This policy has been designed to prepare The Wisdom Council (TWC) to cope with the effects of an emergency. It is intended that this document will provide the basis for a relatively quick and painless return to "business as usual" regardless of the cause.

The objective of this policy is to provide a flexible response so that TWC can:

- Respond to a disruptive incident (incident management)
- Maintain delivery of critical activities/services during an incident (business continuity)
- Return to 'business as usual' (resumption and recovery)

Critical function analysis and recovery process

Priority	Critical function	Timeframe
1	**Office 365 (inc. SharePoint)** **Role responsible**: Director / Technology & Platforms Manager **Likelihood of interruption**: Very Low **Recovery process**: Reach out to our external IT function for them to assess the situation and then raise the issue with Microsoft.	Less than 24 hours (can vary)
2	**Ex-Plor & Recollective (Community Platforms)** **Role responsible**: Director / Technology & Platforms Manager **Likelihood of interruption**: Medium **Recovery process**: Reach out to our relevant contacts at Ex-Plor and Recollective, relay any information about the incident and ask them to escalate.	Varying depending on issue identified, but majority less than 24 hours
3	**Customer Relationship Management Software (HubSpot & FreshDesk)** **Role responsible**: Associate Director **Likelihood of interruption**: Very Low **Recovery process**: Reach out to HubSpot and FreshDesk for a data backup and wait for any issues to be fixed.	Less than 24 hours (can vary)
4	**The Wisdom Council Website** **Role responsible**: Associate Director **Likelihood of interruption**: Medium **Recovery process**: Retrieve back up from SiteGround (website host) and deploy to live site.	2 hours

Emergency Checklist

This table should be used as a checklist during the emergency.

Task	Completed (date, time, by)
Actions within 24 hours:	
Liaise with emergency contacts or services (if required).	

Identify and quantify any damage to the organisation, including staff, premises, equipment, data, records, etc.	
Assess the key priorities for the remainder of the working day and take relevant action.	
Inform staff what is required of them.	
Identify which critical functions have been disrupted.	
Convene those responsible for recovering identified critical functions, and decide upon the actions to be taken, and in what time-frames.	
Provide information to: • Staff • Suppliers and customers • Insurance company	
Publicise the interim arrangements for delivery of critical activities. Ensure all stakeholders are kept informed of contingency arrangements as appropriate.	
Recover vital assets/equipment to enable delivery of critical activities. The essential equipment/resources/information that need to be recovered where possible are: • IT Assets • Office 365 / SharePoint Data • HubSpot Data • FreshDesk Data	
Daily actions during the recovery process:	
Convene those responsible for recovery to understand progress made, obstacles encountered, and decide continuing recovery process	
Provide information to: • Staff • Suppliers and customers • Insurance company	
Provide public information to maintain the reputation of the organisation and keep relevant authorities informed	
Following the recovery process:	
Arrange a debrief of all staff and identify any additional staff welfare needs (e.g. counselling) or rewards	
Use information gained from the debrief to review and update this business continuity management plan	

Contact List

This section contains the contact details that are essential for continuing the operation of the organisation.

Name	Job Title	Contact Number	Organisation
Alison Malton	Director	07900 916150	The Wisdom Council
Nilza Anibal	Technology & Platforms Manager	077079 48803	The Wisdom Council
Martha Webb	Associate Director	07581 524021	The Wisdom Council
Chloe Emerson	Head of Project Management and Onboarding	0113 288 5797	ResearchBods (STRAT7)
Darren Mills	Support Engineer	020 7751 0148	InHouse IT

5. Supplier Management

The following process shall apply to the appointment and ongoing monitoring of all third party suppliers.

1. All new suppliers must be approved at the Management Meeting including by at least 1 Director. Any supplier where the annual contract amount is anticipated to exceed £20,000 must be approved by the Directors.
2. Appropriate due diligence will be completed on all new suppliers including references, financial due diligence and where relevant, data protection and business continuity checks.
3. A register of key suppliers will be maintained. The supplier list should key contact details, nature of services, key contacts, TWC supplier manager and latest supplier review and sign off.
4. All suppliers should have a contract/legal agreement in place, preferably our standard supplier agreement. All legal agreements must be approved by a Director.
5. Any supplier that is a sub-processor of personal data on behalf of TWC and/or TWC clients must have a Data Privacy Agreement in place, approved by TWC legal advisers.
6. Regular service reviews should be completed on all suppliers either on a periodic basis or on completion of projects as appropriate. The review should include at a minimum confirmation of performance against key contractual objectives/service levels.
7. All registered suppliers will be reviewed at least annually. The review should /be completed by the relevant supplier manager and should be updated on the register. The review should be documented on file and should include service reviews, an update on supplier due diligence