Auntie's Cookery Academy

IT Disaster Recovery & Cyber Security Plan

1. Purpose

This plan sets out how Auntie's Cookery Academy (ACA) protects, recovers, and continues operations following:

- A cyber security incident (e.g. phishing, account compromise, ransomware)
- Loss, theft, or corruption of personal or sensitive data
- Loss of access to core IT systems

The plan prioritises the protection of **personal and special category data relating to vulnerable young people aged 18–25**, and ensures compliance with UK GDPR, the Data Protection Act 2018, and insurer expectations.

---

2. Scope

This plan applies to:

- All digital records held by ACA, including learner, safeguarding, staff, volunteer, financial, and governance data
- Google Workspace (email, Drive, Docs, Sheets)
- All devices authorised to access ACA systems (trustee-managed devices only)

ACA does **not** permit the storage of personal data on personal devices or personal cloud accounts.

---

3. Critical Systems & Data

ACA's critical IT assets are hosted within **Google Workspace** and include:

- Learner records (referrals, attendance, safeguarding concerns, Individual Safety Plans)
- Staff, volunteer, and trustee records (DBS status, training, contact details)
- Financial records (budgets, invoices, donor information)

- Governance documents (policies, board minutes, risk register)
- Official ACA email communications

Approval Date	09.12.25
Next Review Due	09.12.26
Version Number	1.0

Loss, unauthorised access, or corruption of this data would create **safeguarding, legal, and reputational risks**.

---

4. Data Storage & GDPR Controls

ACA relies exclusively on **Google Workspace's secure cloud infrastructure**.

Controls in place:

- Data is stored in structured Google Drive folders with restricted access
- Safeguarding and sensitive learner records are held in a **dedicated secure folder**
- Access is limited to Trustees only, on a role- and need-to-know basis
- Sharing permissions are disabled by default and reviewed regularly
- All data transfers occur through encrypted connections

ACA follows GDPR principles of data minimisation, confidentiality, and purpose limitation.

---

5. Backup & Data Recovery Strategy

5.1 Backup Method

- Google Workspace's automatic data replication and redundancy is relied upon as the primary backup mechanism
- File version history and restore functions are enabled for all Drive documents
- Deleted files are recoverable within Google's retention periods

5.2 Backup Frequency

- Operational and safeguarding data: Continuous backup via Google's infrastructure
- Financial records: Maintained within Drive with version control
- Governance records: Backed up automatically and following major updates

5.3 Access to Backups

- Only Trustees retain administrator privileges
- Admin credentials are secured with strong passwords and multi-factor authentication
- Recovery options are reviewed annually

---

6. Cyber Security Measures (Prevention)

ACA applies proportionate cyber security controls consistent with insurer and ICO expectations:

- Google Workspace admin accounts protected with multi-factor authentication
- Strong password policies enforced
- Limited admin access (Trustees only)
- No use of personal email or storage for ACA business
- Automatic security updates enabled on all authorised devices
- Awareness of phishing and social engineering risks embedded into trustee and staff induction
- Regular review of user access permissions

ACA does not allow volunteers or third parties unsupervised system access.

---

7. Incident Response Procedure

Step 1 – Immediate Containment

- Lock or suspend compromised Google accounts
- Remove affected user access
- Preserve evidence (emails, logs, file versions)

Step 2 – Internal Notification

- Incident reported immediately to the CEO
- CEO assesses scope, data types involved, and safeguarding implications
- Trustees notified promptly where risks are material

Step 3 – Risk Assessment

- Determine whether personal or special category data is affected
- Assess impact on learners, particularly safeguarding risks
- Identify if data has been accessed, altered, or exfiltrated

Step 4 – External Reporting

Where legally required:

- Notify the Information Commissioner's Office (ICO) within 72 hours
- Notify affected individuals if there is a high risk to rights or safety
- Liaise with police or the National Cyber Security Centre where criminal activity is suspected

---

8. Recovery & Restoration

ACA will:

- Restore data using Google Workspace recovery tools and file version history
- Reset passwords and force re-authentication where required
- Review permissions and admin access
- Confirm data integrity before resuming normal operations

Recovery objectives:

- Essential systems operational within 48 hours
- Full recovery within 5 working days where feasible

---

9. Safeguarding & Sensitive Data

Where incidents involve safeguarding records or vulnerable learners:

- Protection of learners takes precedence over system recovery speed
- Access to sensitive folders is restricted further during investigation
- Safeguarding partners are notified if risk thresholds are met
- Actions are documented and retained securely

---

10. Roles & Responsibilities

- **CEO**: Overall responsibility for IT security, breach decisions, and reporting
- **Trustees**: System administration, oversight, and assurance
- **All staff and volunteers**: Must follow data protection procedures and report concerns immediately

ACA does not currently outsource IT support; external expertise may be sought during serious incidents.

---

11. Training & Awareness

- Trustees and staff receive data protection and cyber awareness guidance
- Key risks are embedded in induction and reviewed annually
- Cyber and data risks are recorded in the Risk Register

Approval Date	09.12.25
Next Review Due	09.12.26
Version Number	1.0

12. Insurance & Compliance Alignment

This plan supports:

- Cyber and data protection insurance requirements
- Charity Commission expectations for risk management
- ICO guidance on data security and breach response

---

15. Policy Review

This policy will be reviewed **at least once every 12 months**, or sooner if:

- Relevant laws, regulations, or guidance change;
- A serious incident, complaint, or near miss occurs;
- Feedback from learners, staff, or partners suggests improvements; or
- Operational changes make an update necessary.

This includes review following changes in ICO guidance or data breach incidents.

Signed: 

Printed Name: Emily-Jane Dale
Job Title: CEO and Chair
Date: 9th December 2025

Approval Date	09.12.25
Next Review Due	09.12.26
Version Number	1.0