The Resource Centre, Sandgate, Penrith CA11 7TP

Landline: 01768 867629
Mobile: 07554 370823

Registered Charity No. 1177317

High Sheriff Award 2020
Police & Crime Commissioner Outstanding Community Project Award 2020
FCSCT Peter Scott Award for Outstanding Contribution to Charity 2019
Diverse Cumbria Community Group Champion of the Year 2017

Information Security Policy

Updated Dec 2025

Contents

1. Introduction

The information Triple A holds and the Information and Communications Technology (ICT) systems and networks that support it are important business assets. Many potential threats to these exist, such as fraud, vandalism, virus infection, theft, loss, abuse of copyright, misuse of software and accidental damage. The International Standard: ISO 27001:2013 Code of Practice defines Information Security as the preservation of:

- **Confidentiality**: ensuring information is accessible only to those authorised to have access;
- **Integrity**: safeguarding the accuracy and completeness of information by protecting against unauthorised modification; and
- **Availability**: ensuring information and services are available to authorised users when required.

Triple A is committed to preserving the confidentiality, integrity and availability of our information assets:

- For sound decision making
- To deliver quality services
- To ensure data quality and accurate, up-to-date, information
- To comply with the law
- To meet the expectations of our service users
- To protect our service users, staff, contractors, partners and our reputation as a professional and trustworthy organisation
- To support flexible, remote and home working
- To enable virtual meetings
- To ensure Triple A can continue working without interruption
- To enable secure and appropriate sharing of information.

2. Scope

This Policy is mandatory and there are no exceptions to it. It applies to all employees of Triple A, including temporary and contract staff (including agency staff), contractors, agents and partners, who have authorised access to Triple A's IT systems.

This Policy applies throughout the lifecycle of information held by Triple A on all types of media, from its receipt or creation, storage and use, to disposal.

3. Policy Statement

Triple A understands the importance of information security and privacy. We are increasingly dependent on ICT systems and so the potential impact of any breach is also increasing. We must safeguard our information systems and ensure compliance with this Policy, to provide protection from the consequences of information loss, damage, misuse or prosecution.

The General Data Protection Regulation (GDPR) places a duty on Triple A to demonstrate accountability and to have in place the organisational and technical measures to protect the personal data it holds and processes. We are committed to providing the levels of information security required to protect this data and this Policy helps to set out how we aim to achieve the necessary standards.

We also aim to fulfil the business needs of Triple A and to allow people to work in a flexible way, whilst maintaining the security levels required.

4. Legal and Regulatory Requirements

Triple A has an obligation to ensure all its information systems and information assets and users of those systems and information assets comply with the following:

- Civil Contingencies Act 2004
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Data Protection Act 2018
- Electronic Communications Act 2000;
- General Data Protection Regulation (GDPR)
- Privacy and Electronic Communications Regulations 2003 and EPrivacy Regulation 2018
- Public Services Network Compliance
- Telecommunications (Lawful Business Practice) Regulations 2000.

If you are unsure about the relevant legal or regulatory requirements relating to the information you use in your work, please contact the Chief Executive for guidance.

5. Controls

Triple A has information security measures in place to help mitigate risk, known as controls. These controls are divided into three categories: administrative, technical and physical.

5.1 Administrative Controls

5.1.1 Policies and Authorised User Agreements

This written Information Security Policy document is available to all with authorised access to Triple A's IT systems. Authorised users are required to read this document and also the 'Internet and Email Acceptable Use Policy.'

- All authorised users must sign the ICT Authorised User Agreement to indicate their acceptance of these policies, before access to Triple A's equipment, network and systems can be granted.
- A process of regular acknowledgement of Triple A's information security policies by all authorised users is in place.

5.1.2 ICT assets - classification and control

Triple A's ICT infrastructure is such that almost all components are considered to be part of a single network, with a separate network for guest access. Triple A uses a number of cloud based services all of which meet the security standards required within Triple A's cyber essentials certification.

- No computer, device or hardware shall be acquired or connected to the network and no software shall be installed onto Triple A's network or procured (with a view to being installed), without prior approval from IT Services.

Assets are things of value. Triple A has many ICT assets and this Policy aims to protect those related to Triple A's network. Triple A are responsible for maintaining a database of all ICT assets. This describes the assets, who they are allocated to and records any authorised uses and security procedures related to them.

ICT assets are allocated to an individual, who has use of and is responsible for them. Staff who use portable corporate devices, such as laptops, iPads, tablets and mobiles, must be particularly vigilant, since these devices are more likely to be lost, damaged, or stolen. ICT assets are regularly audited to ensure that no breaches of the Information Security Policy are taking place.

- Corporate portable devices must not be left unsecured in public places.
- Corporate equipment must not be taken abroad unless permission is approved by the Chief Executive.

5.1.3 Information security education and training

Triple A will seek to provide authorised users with appropriate training, including information security. It is the responsibility of line managers to ensure that staff undertake the training provided

All new employees are made aware of this Policy and asked to sign it as part of their induction.

5.1.4 Prevention of misuse of ICT facilities

Triple A permits authorised users the use of corporate ICT equipment and systems for managed personal use, but this must be in their own time.

- Triple A's ICT equipment and systems must not be used for the conduct of personal purposes during working hours, or under any circumstances for private commercial activity. Failure to comply may result in disciplinary action.

5.1.5 Contracts with data processors

Whenever Triple A enters into an arrangement with a data processor who will have responsibility for holding and/or processing Triple A's data, including personal data, a formal contract containing appropriate safeguards shall be drawn up between that data processor and Triple A.

5.1.6 Reporting security incidents

- All security incidents and breaches must be reported immediately. All authorised users have a responsibility to promptly report any suspected or observed incident or data breach.
- Incidents or breaches that result from deliberate or negligent disregard of any security policy requirements may result in disciplinary action being taken.

All incidents will be logged and reviewed, so that they can be effectively managed and lessons learned.

5.1.7 IT Disaster Recovery Plan and business continuity

It is the responsibility of the Chief Executive to prepare and test an IT Disaster Recovery Plan or to outsource this to an appropriately quali8fied organisation. The Plan identifies the risks to information and services and steps for reducing those risks and mitigating the potential impact of various types of disaster on business activities.

5.1.8 Control of proprietary software copying

Authorised users must not:

- copy licensed software, install or use unlicensed software. Software is protected by copyright.
- download material such as fonts, drivers, shareware, or freeware, without proper authorisation from IT Services.
- copy or download material or publish it on Triple A website, unless they have permission to do so. Much of the material on the internet is protected by copyright.

Triple A retains copyright and intellectual property rights over material produced in the normal course of an authorised user's employment, engagement, or association.

5.1.9 Data protection

Personal information on living individuals (who may be identified from the information held) is subject to the Data Protection Act 2018 and GDPR. Compliance with Data Protection legislation is the responsibility of Triple A's Data Protection Officer. Authorised users must be aware of their responsibilities for personal data and that training is available. Further guidance can be obtained from the Data Protection Officer.

- In the event of needing to share personal data with a contractor or other third party, appropriate safeguards must be written into the contract. If there is no formal contract in place, a Data Sharing Agreement must be completed and signed by all relevant parties.

5.1.10 Safeguarding of organisational records

Important records of the organisation should be protected from loss, destruction and falsification.

5.1.11 Virtual meetings

Triple A uses Microsoft Teams and Zoom conferencing technology for the holding of its virtual meetings. All authorised users are required to follow the guidance below when taking part in virtual meetings:

- When hosting an online virtual meeting, only do so with Triple A's corporate account. Personal accounts are not appropriate for this purpose.
- If unsure, check with the host that a meeting is being hosted by a corporate/paid-for account. Free versions of software are often less secure than corporate/paid-for versions and carry increased security risks as a result.
- Do not say anything you would not want to be recorded or transcribed.
- Do not assume everything shared in a virtual meeting is coming from a valid source.
- Do not assume that everyone at a virtual meeting is there is for a valid purpose.
- As with email, do not open files from untrusted sources.
- Check that the meeting links you receive are from people you trust.
- Remember to check that no sensitive information could be visible, before sharing screens.

- Take care not to share sensitive documents with meeting attendees from outside the organisation who should not have access to them.

5.2 Technical Controls.

5.2.1 Access controls and passwords

System access control is achieved through applying access rights and the use of unique usernames and passwords. Security of passwords is essential. Each authorised user is responsible for the security of their passwords:

- Do not let anyone else know your passwords. Choose a secure password that is hard for others to guess.
- Do not leave a computer that is logged into the network unattended without first locking your screen.

5.2.2 Encryption

All of Triple A's laptops and portable corporate devices should be encrypted.

5.2.3 Patches and updates

Triple A's computers must be properly patched with the latest appropriate updates, to

reduce system vulnerability and enhance and repair application functionality. It is the responsibility of the user to apply these updates to their own devices. If guidance is needed on this it can be sought through the Chief Executive or Executive Assistant.

5.2.4 Virus controls

Triple A are responsible for engaging suitably qualified persons to implement and monitor anti-virus measures to protect Triple A from computer virus infections and other harmful programs.

- If you suspect the equipment you are using may be infected, switch off and disconnect from the network. When this is done, inform your line manager and report to IT services immediately.
- Personal devices - may not be as well protected as corporate devices and, if infected with a virus, could infect a corporate device. These should not be used for Triple A work unless the company portal is installed and all work-related files and data remain within this.
- Never connect non-corporate devices (any form of removable media) to a corporate device, or to the corporate network.
- Portable memory devices – encrypted devices should be used where possible.
- Email - email itself is rarely harmful; it is primarily documents, links in emails and programme attached to emails that can contain viruses. If you don't recognise the sender, or have any doubts at all about an email, do not open it; it is better to delete it.
- Never open attachments or click on links within an email unless you are certain you know where the email has come from.
- Websites - are another source of viruses. Triple A's anti-virus software should automatically detect any viruses before anything is downloaded. If you see a warning message, leave the website and contact your line manager. Be vigilant when browsing the internet and accessing web-based personal email systems using corporate equipment.

If a computer virus is transmitted to another organisation, Triple A could be held liable if there has been negligence in allowing it to be transmitted. So always take care, do not open anything suspicious and, if in any doubt, contact your line manager.

5.2.5 Transferring data

Where restricted, confidential, or sensitive data needs to be sent outside of Triple A, a secure method must be agreed and documented, in consultation with the Chief Executive.

- Under no circumstances must any restricted, confidential, or sensitive data be copied to any form of removable media.
- Do not use non-corporate devices, such as personal USB memory sticks, to transfer information from, or to corporate devices, or the corporate network.

6. Compliance with the Information Security Policy

The implementation of this Policy will be monitored to ensure compliance. An audit of software and hardware will be conducted on a regular basis by an appropriately qualified third party.

Any breach of this Policy by staff may lead to disciplinary action.

7. Review

This Information Security Policy will be reviewed by the Chief Executive and Board of Trustees, and updated by December 2026.