

# IT Management Policy

---

## Purpose

This policy details standards and practices for the management of IT systems under the control of 2<sup>nd</sup> Acomb Scout Group.

## Applies to

All adult members of 2nd Acomb Scout Group who control or administer IT systems used for Group purposes.

## Summary

The policy sets out how 2nd Acomb Scout Group selects, configures and manages its IT systems to ensure security, compliance, integrity, reliability and cost efficiency. It details the responsibilities of the IT Team and any other administrator of IT systems, and approved systems which must be used for core purposes.

It requires strong access controls, unique user accounts, robust password and MFA requirements, encryption, regular software updates, secure system disposal, Single Sign-On where possible, and adherence to the principle of least privilege. The policy enforces consistent standards across all platforms – covering email, document storage, communications, member management, domains, and website hosting. It also ensures Group ownership of accounts and domain registrations, prioritises UK/EU data sovereignty, and mandates consultation with the IT Team before introducing or changing any system.

## Contents

IT Management Policy .....	1
Purpose .....	1
Applies to .....	1
Summary .....	1
Contents .....	1
Version control .....	2
Principles .....	2
IT Team .....	3
System configuration standards .....	3
Account naming .....	3
Passwords .....	3
Principle of Least Privilege .....	4
Single Sign-On .....	4

Other account protections .....	5
Account closures.....	5
Encryption.....	5
Devices.....	5
Backups.....	5
Software updates.....	5
Ownership of accounts and domain names .....	5
Data sovereignty .....	5
Cost control .....	5
Disposal.....	5
Core platforms.....	6
Email .....	6
Document and data storage .....	6
Messaging and conferencing .....	6
Member management.....	6
Social media.....	6
Domains and DNS .....	6
Website hosting.....	6
Legacy configuration.....	6

## Version control

Version	Author	Role	Release date
1.0	Russell Odom	Deputy Chair	10 Feb 2026

## Principles

2<sup>nd</sup> Acomb Scout Group use many different IT systems, both directly managed and managed by third parties, in the course of providing our mission of Skills For Life for our young people.

It is our policy that our selection, configuration, administration, use and disposal of all such systems, by any member of the Group, must be carried out in a way that keeps those systems and the data stored therein intact, secure, available, reliable, performant, in compliance with our legal responsibilities and the requirements of The Scout Association, and giving good value for money.

This policy applies to the management of any IT system which is procured by the Group and used for Group purposes, including social media accounts and third-party products and services. All members of the Group who manage, administer or control such systems are responsible for adherence to this policy.

## IT Team

The Group has an IT Team who take primary responsibility for management of systems under direct control of the Group, and provide help and advice for other systems. Members of this team will have sufficient skills and experience to undertake this role, and must exercise the responsibility to the best of their abilities. This team is responsible to the Group Trustee Board.

Other systems may be administered by other members of the Group, but still in compliance with the standards in this policy.

The IT Team must be consulted before any new IT system, for any Group purpose, is purchased or otherwise brought into use, and before any proposed major change to the Group's use of existing systems. They will vet the system for suitability according to this policy, and may veto or impose conditions on its use, or refer decisions to the Group Trustee Board where appropriate for reasons of cost or risk.

## System configuration standards

When configuring and managing Group systems, as far as is possible within the constraints of the system concerned, the following standards should be adhered to.

When evaluating new systems for use by the Group, their ability to be configured to adhere to these standards must be taken into consideration.

### Account naming

Accounts on systems used for Group purposes **must not be shared** between multiple people unless it is unavoidable due to system limitations. Each account must be identifiable to the specific individual who owns it.

Usernames/email addresses in M365 should be of the form *firstname.lastname@domain*. Other addresses specific to that individual (Scouting name, nickname, Trustee Board role name, and similar, e.g. "akela@" or "chair@") are added as aliases on the account. Team or shared role addresses should be created as Distribution Lists, Groups or shared mailboxes.

Usernames on other systems should be the *firstname.lastname@domain* email address, or *firstname.lastname* if email address is not possible.

Individuals should not have more than one account on any system.

### Passwords

Passwords used on any account on any system must be **unique** to that user on that system; **passwords must not be reused** on any other system, within the Group or otherwise.

Passwords should be at least **12 characters long** and must not be readily guessable. There is no requirement of complexity or special characters, but it is strongly recommended that password be either:

- randomly generated and stored in a password manager; or
- formed of a sequence of three or more random words which are easily remembered<sup>1</sup>

Passwords will have **no** requirement to be changed on a regular basis; a password change will only be required if there is a suspicion or indication of compromise of the password.

Passwords to an account may only be disclosed to the account owner on initial creation, change of ownership of an account, or administrator reset; the new owner must be required to change any such password on next login. They may also be shared, securely, where system limitations mean shared accounts must be used.

---

<sup>1</sup> See <https://xkcd.com/936/>

Passwords may not be shared with any other person under any other circumstance, nor stored insecurely. Care must be taken to verify the identity of the user before sharing.

#### Password resets on request

Where possible, systems should be configured to allow users to reset their own passwords, via security questions or alternative communications routes such as an email or text message.

An administrator may reset a password on request of the user only once that user's identity has been **positively verified** via already-known information.

#### Actions on password/account compromise or device loss

In the event of a being notified of a compromise, or suspected compromise, of any account or password on any Group system, the IT team must, as soon as reasonably practicable:

- If not already done, change/invalidate the password, or contact an administrator of the system to do so
- Where possible and not already done, revoke any current authenticated sessions for the account (to require re-authentication with the new password)
- Assess the circumstances, risk and impact, and
  - Communicate any non-trivial incident to the Group Lead Volunteer and Group Trustee Board
  - Communicate any potential data breach (with regard to the Data Protection Policy) to the Data Protection Lead
  - Take any other actions they deem necessary to secure the account, other accounts belonging to the user, and any other Group IT system
  - Raise any remaining risk they identify in accordance with the Risk Policy

A loss of a Group-managed device, or a personal device containing Group data or credentials, should be treated as a potential compromise of account credentials on all systems to which the device may have had access, and acted upon as above. The response must also consider what data may have been stored on the device.

#### Multi-factor authentication

Within the capabilities of individual systems, use of multi-factor authentication (MFA/2FA) must be allowed for all accounts on any system used for Group purposes, and is **required** in these cases:

- Any administrative-level account on any system
- Any account in the M365 tenancy with access to SharePoint or OneDrive
- Any account which has access to Personal Data or confidential information

Where possible, systems must be configured to require multi-factor authentication for appropriate users in these circumstances.

#### Principle of Least Privilege

Where available, the permissions associated with any account on a Group IT system must be set to the least required for the role of the person who owns it.

Wherever possible, permissions must be administered by membership of roles/groups rather than assigning individual permissions direct to an account.

#### Single Sign-On

Wherever possible, Group IT systems should be configured with Single Sign-On, authenticated against the Group M365 tenancy.

### Other account protections

Where possible, system features should be enabled to further protect accounts; these may include feature such as geographical restrictions (allow UK logins only; exceptions can be made on an individual basis as required) and disallowing poor quality or known compromised passwords.

### Account closures

Anyone leaving the Group must have their accounts on Group IT systems removed **as soon as reasonably practicable**. Their manager is responsible for informing the IT Team of their departure and ensuring removal from any system not managed by the IT team. The IT team are responsible for removing accounts from directly-managed systems.

### Encryption

All information must be encrypted in transit and at rest, to modern encryption standards.

### Devices

Any computing device owned by the Group must have logins tied to the M365 tenancy where possible. Storage should be encrypted. Suitable endpoint protection (including anti-virus and remote management) should be configured.

### Backups

Where appropriate, backups of any managed system should be taken on a regular, automated basis. The method, destination, frequency, and retention period are to be assessed by the IT Team and implemented on a case-by-case basis.

### Software updates

The IT team should apply software updates a timely fashion on any directly-managed system. Where possible, systems should be configured to apply updates automatically.

### Ownership of accounts and domain names

System tenancies, account ownerships, domain names and other registrations are always to be registered in the name of the Group, not in the name of an individual. The registered email address should be [IT@2ndacombscoutgroup.co.uk](mailto:IT@2ndacombscoutgroup.co.uk) or, in appropriate circumstances, another role-based Group email address (e.g. *chair@domain* - addresses for a named individual are not to be used). This is to allow the Group to retain access if an individual leaves the Group or moves roles.

Domain name registrations must use a registrar account under control of the IT Team.

### Data sovereignty

Data and services should be physically located within the UK, the EU where this is not possible, and other countries only where the provisions of the UK Data Protection Act ("GDPR") can be applied on an equivalent basis.

### Cost control

Systems should be configured in a cost-effective manner and pricing plans selected at the lowest level which meets Group requirements. Where pricing is variable, notifications should be configured to detect unusually high costs. Spending must be approved in compliance with the Finance Policy.

### Disposal

On disposal or end of use of any Group system, all data therein must be wiped/removed/deleted to the most full and secure extent reasonably possible, and the account/tenancy itself deleted, as soon as reasonably practicable.

## Core platforms

The following core platforms have been selected for use by the Group and may not be changed without a robust selection process and approval of the Group Trustee Board. The Data Protection Policy must be updated to reflect the new systems where appropriate.

### Email

Group email is hosted on Microsoft's M365 platform. Every adult member of the group will be allocated a Group email address to use for Group purposes.

### Document and data storage

The primary store for Group documents and other information is on SharePoint or OneDrive in the Group's M365 tenancy. Other systems may be used only where the information is appropriate to the specific purpose of that system.

### Messaging and conferencing

For Group purposes, messaging and conferencing between more than two members of the Group, or from the Group to parents/guardians, should use:

- MS Teams under the Group M365 tenancy; or
- WhatsApp in a group under one of the 2<sup>nd</sup> Acomb communities

### Member management

The Group uses Online Scout Manager (OSM) for the purposes of storing member data, managing and communicating with members, and managing events and programmes.

### Social media

The Group uses the following social media services:

- Facebook
- Instagram

### Domains and DNS

The Group uses GoDaddy for domain registration and DNS management. AWS is used for Redmire only.

### Website hosting

The Group uses GoDaddy for website hosting. AWS is used for Redmire only.

## Legacy configuration

The Group Trustee Board recognise that historical practices, before creation of this policy, in many cases do not follow the requirements laid down herein. The IT team and other members of the group with IT administration responsibility will work to bring all configuration into compliance as far as is reasonably possible, as time and circumstances allow; this process will be managed under the Risk Management Policy.

Where any configuration cannot reasonably be amended, any specific risks identified as a result will be recorded and managed as per the Risk Management policy.