

IT Usage Policy

Purpose

This policy details standards and practices for the use of IT systems under the control of 2nd Acomb Scout Group.

Applies to

All adult members of 2nd Acomb Scout Group.

Summary

The policy sets out how members of 2nd Acomb Scout Group use Group IT systems responsibly, including using official Group email accounts, storing data only in approved locations, using strong unique passwords, and enabling multi-factor authentication. It prohibits misuse such as sharing confidential data, accessing unsuitable websites, or using systems for non-Group purposes. The policy also sets rules for supervised internet access for under-18s, restricts official social media activity to approved accounts, and permits the use of AI tools only without uploading personal or sensitive information. The IT Team oversees systems, approves new tools, and provides support.

Contents

IT Usage Policy	1
Purpose	1
Applies to	1
Summary	1
Contents	1
Version control	1
Principles	1
Security and compliance	1
Email	2
Document, data and media storage	2
Passwords	2
Password compromise	2
Multi-factor authentication	2
Responsible usage	3
Internet access	3

Under 18s internet usage	3
Social media and messaging	4
Personal device security	4
Use of AI.....	5
IT Systems Management	5
Help and support	5

Version control

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

Principles

2nd 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 use of all such systems must be carried out in a way that keeps those systems and the data stored therein intact, secure, available, reliable, performant, and in compliance with our legal responsibilities and the requirements of The Scout Association.

Security and compliance

Email

To retain control of Group data, every adult member of the group **must use their allocated a Group email address for Group purposes**; use of personal or non-Group email addresses for Group purposes is not permitted.

In particular, no non-public Group file/document may be attached and sent from or to any personal address of a Group member.

Document, data and media storage

The primary store for general Group documents is on SharePoint or OneDrive in the Group's M365 tenancy. Documents may be stored in other Group systems where appropriate to the purpose.

To comply with our Data Protection Policy, **no non-public Group document may be stored on, or shared from, personal devices or non-Group systems** unless a temporary local copy (which must be deleted as soon as possible) is required for technical reasons, such as transfer between systems.

Wherever possible, documents must be shared by link to M365 rather than as direct attachments.

Photographs/videos of Group events on leaders' personal devices are an exception to this requirement, as set out below and in the Data Protection Policy.

Passwords

Passwords used on any account on any system must be **unique** to your account on that system; **passwords must not be reused** on any other system, within the Group or otherwise. This is to reduce the risk of a

compromise of one system leading to compromise of other systems (this is the most common cause of IT security incidents).

Passwords should be at least **12 characters long** and must not be readily guessable. There are generally no requirements to use mixed case, numbers, or special characters – longer passwords have been shown to be more secure than shorter, more complex ones¹. A good approach is to pick 3 or more random but memorable (to you) words. Alternatively, you can generate and store long random passwords with password manager software. You will NOT normally be required to change passwords on a regular basis.

Passwords for an individual account must not be shared with any other person.

Password compromise

Any member who knows or suspects any password on any Group system has been disclosed or compromised must, as soon as reasonably practicable:

- **Change the password** on the affected account, if they are able to access it; and
- Where the system allows it and they are able to do so, revoke any sessions currently active on the account (to force a re-login); and
- **Inform the IT Team** by email to IT@2ndacombsacoutgroup.co.uk
 - If this is not possible, then direct or indirect contact via other means (e.g. phone call, text message, WhatsApp, or via another person) is acceptable, but they must keep trying until they receive an acknowledgement from a member of the IT team.

Multi-factor authentication

Use of multi-factor authentication (MFA/2FA) is **strongly encouraged** for all accounts on any Group IT system. Multi-factor authentication is **required**, wherever the system allows it, 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

Responsible usage

No member of the Group may use any Group IT system in any way which is illegal, not in accordance with POR, Scout Association guidance, the principles of Scouting, or such that it may bring the Group or Scouting into disrepute. Terms of Service for all systems must always be followed.

Unacceptable use of the Group IT systems includes, but is not limited to:

- Sending or posting discriminatory, harassing, or threatening messages or images on the internet or via the Group's email service
- Using computers to perpetrate any form of fraud; software, film or music piracy, copyright infringement or other criminal activity
- Stealing, using, or disclosing someone else's account, resources or password without their authorisation
- Sharing confidential or sensitive material outside of the organisation

Group IT Systems must only be used for Group purposes.

Members must not incur excessive costs on any Group IT system, nor use systems in ways which impair the performance, security integrity or availability of the system for any other user.

¹ See <https://xkcd.com/936/>

Under no circumstances must users attempt to circumvent any restrictive system configuration or requirement which may have been added by an administrator; such restrictions are in place for good reasons.

Internet access

Use of the internet via 2nd Acomb Scout Group IT systems (i.e. the Wi-Fi connection at any Group premises) is permitted and encouraged where such use supports the goals and objectives of the group. However, this access is a privilege; users are expected to use the internet responsibly and productively and adhere to this policy.

Note that:

- All Internet data that is composed, transmitted and/or received by 2nd Acomb Scout Group's computer systems is considered to belong to the Group and is recognised as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties.
- The equipment, services, and technology used to access the internet are the property of 2nd Acomb Scout Group, and the Group reserves the right to monitor internet traffic and monitor and access data that is composed, sent or received through its online connections.
- Emails sent via the Group email system must not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images.
- All sites and downloads may be monitored and/or blocked by 2nd Acomb Scout Group if they are deemed to be harmful and/or not productive to the group.

Under 18s internet usage

All adults are to be aware that the internet feed is unfiltered.

- Nobody under the age of 18 should have access to the Wi-Fi password
- Every child under the age of 18 is to be supervised at all times when accessing the internet or working with Group IT equipment
- Any young person seen to be trying to access social media or any other unsuitable websites will be stopped and reminded of their behaviour and this logged on OSM and the section leader informed

When under 18s are permitted by their Leader to bring mobile phones/devices to an activity, this is done so with permission of their parent/guardian. Leaders are not responsible for monitoring/supervising their content/usage but will remind them of the no social media/suitable website rules. If unacceptable use is brought to their attention, they will respond as stated above. The device may be removed for the duration of the activity and returned to parent/guardian when the under 18 is collected.

Social media and messaging

Only official Group accounts on approved social media services (Facebook and Instagram, as listed in the IT Management Policy) may be used for official Group purposes. No new account on these services may be created for Group purposes unless approved by the Leadership Team or Group Trustee Board. Members using these accounts must have completed any relevant training, and do so in accordance with The Scout Association's social media policy.

Personal social media accounts may not be used to post any official Group information or announcements (but may re-share official information). You may promote or indicate your membership of the Group on your personal social media accounts, provided it is clear that any related post is in a personal capacity, not an official communication, and that your account does not in any way bring the Group or Scouting into disrepute.

Only approved messaging apps and systems (primarily WhatsApp and OSM, but including any other app/system listed in the IT Management Policy) may be used for communication with parents/guardians.

Photographs and videos taken at Group events must only be handled and shared on social media and in messaging apps in accordance with the Data Protection Policy, with a device meeting the standards set out below.

Personal device security

Where a personal device (phone, PC, laptop, tablet, etc.) is used for to access Group systems or for Group purposes, it must meet the following standards:

- Supported by the vendor and receiving timely security updates
- Encrypted storage (all Android and iPhones have this; Windows and Mac may not have it turned on by default)
- Password/PIN/pattern (not shared with anyone else) or biometrics required to unlock

Where a device contains any Group data (temporary document copies, photographs/videos as allowed in this policy, emails, or saved credentials), care should be taken not to leave it unlocked or unattended in a public space. Any loss/theft must be reported to the IT team (as earlier in this document) as soon as reasonably practical. The IT Team will then take action to protect your accounts and assess other risks, as detailed in the IT Management Policy.

The Group recognise that devices may back up data or copy media to services outside Group control. You should be aware of such activity your device performs and take all reasonable steps to keep this secure, and to notify the Group any potential compromise or data breach.

Should you leave the Group, you must delete all Group data, media and credentials from your devices, and any services to which that data may have been copied, as far as reasonably possible.

Use of AI

Members of the Group may use “AI” services for Group purposes. However:

- No Personal Data may be uploaded for processing to any AI service.
- No Group sensitive/confidential information may be uploaded for processing to any AI service, with the exception of Copilot in the Group-managed M365 tenancy.
- Any user of AI should be aware of the possibility of mistakes (“hallucinations”) and must carefully review all output for accuracy, completeness and suitability before relying upon it.

IT Systems Management

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. Other systems may be administered by other members of the Group. Any Group member who has control of, or administration responsibility for, any system must do so in compliance with the IT Management 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.

Help and support

If you have a problem with any Group IT system, or any questions about this policy, you can contact a member of the IT Team at IT@2ndacombscoutgroup.co.uk.