Girlguiding
Anglia

27. Acceptable use policy (AUP)

Ratified: January 2024
Issue: 04
Next Review: 2025

Contents

Please note:

Where there is a reference to internal IT support this is currently Lucy Martin, member support manager, who can be contacted:
E: angliahq@girlguiding-anglia.org.uk P: 01603 737357

Where there is a reference to external IT support team or department this is currently provided by Netmatters, who can be contacted in agreement with your line manager or volunteer office contact:
E: support@netmatters.com P: 01603 704020

Where there is reference to the region data protection officer this is currently Bonnie Dillaway, communications and opportunities manager, who can be contacted:
E: dataprotection@girlguiding-anglia.org.uk P: 01603 737357

1) Statement of purpose

As staff and volunteers who use Girlguiding Anglia digital systems and equipment, it is important you do so in a safe, secure, and appropriate way.

If you are in breach of this policy you may be subject to action under either the Disciplinary Procedure (see Staff handbook – policy 13 Disciplinary Policy and Procedure) or, if you're a volunteer, the Girlguiding Volunteer Code of Conduct.

Is this policy for me?

You must comply with this procedure when using Girlguiding Anglia's digital systems, equipment, and organisational information (including membership data) if you are one of the following (referred to from now on in this policy as 'users'):

- Any employee or contractor of Girlguiding Anglia. This means all:
  - Permanent employees
  - Temporary employees
  - Interns and apprentices
  - Work experience/direct volunteer roles

- A national volunteer in any of the following roles:
  - Chief commissioner (or chief commissioner designate)
  - Deputy chief commissioner (or deputy chief commissioner designate)
  - Assistant chief commissioner
  - Senior/lead volunteers engaged at a regional level
  - A Girlguiding member with a Girlguiding Anglia email address

Whatever your role or reason, if you are using Girlguiding Anglia digital systems and equipment you must use the appropriate starters and leavers process to gain or change access.

Additional note:

All database access to the membership system (GO) is controlled by a separate sign-up process with linked procedures. This is controlled and managed by Girlguiding and subject to its own user agreements. Once data is downloaded from GO to region systems it then falls under this policy and the Managing Information policy.

2) Use of email

Email system
Girlguiding Anglia provides an email system to support charitable and business activities.

- You must make sure all emails conducting or supporting official Girlguiding Anglia business use:
  - An @girlguiding-anglia.org.uk or @hautbois.org.uk address.
  - The Girlguiding Anglia, Hautbois Activity Centre or Girlguiding Anglia retail official signature formats (these are added automatically on sending an email).

  Do not use your personal email account(s) (including ones used for volunteering) to conduct or support official Girlguiding Anglia business. This applies to all users of this policy.

  The use of email facilities that have not been authorised, or any misuse may be considered a breach. This will be dealt with under the disciplinary procedure, or for users gaining access due to their volunteer role, under the Girlguiding code of conduct.

- All emails that represent aspects of Girlguiding Anglia's business or administration are the property of Girlguiding Anglia and not of any individual user. Emails sent or received on Girlguiding Anglia's email system are part of Girlguiding Anglia's administrative records. This means they may be used, stored, and accessed accordingly.

- We have systems in place to filter malicious emails (VIPRE email security). But there may be times when you receive suspicious mail. If you do:

  - Contact the Girlguiding Anglia IT team to report this, they may advise reporting it on to the external IT support team.
  - Do not reply to the emails, click on any links within the email or open any attachments.
  - Do not enter personal details, including usernames and passwords, into any untrusted sources. If you need help to check the source, contact the internal IT support team.
  - Do not give your Girlguiding Anglia email address out without thought. Before giving your Girlguiding Anglia email address to a third party (for example, on an online form or to access WiFi at a venue) consider what the organisation is, and what controls it has in place to protect your email address. What is the possible impact of your address being passed or sold to an unknown third party, do the benefits outweigh the potential problems?
  - You should not use your Girlguiding Anglia email address for non-business purposes, such as signing petitions or commenting on social media.

- **If you believe you have become the victim of a malicious email or clicked an untrustworthy link, immediately remove your internet connection, and contact the region IT department immediately.**

Email content

You must keep your email content secure.

- Always consider who you are sending an email to:
  - Bcc should always be used when contacting multiple people unless agreements are in place for emails to be shared.
  - For emails with a large number of recipients please contact the communications team to discuss the use of DotDigital as an alternative communication tool.
  - Do not share an individual's personal details with a group unless explicit permission is given.
  - You must not contact members under the age of 14 directly. If you are unsure or if you are contacting a group of members, always do so in consultation with the data protection officer.
  - When forwarding an email, remove unnecessary parts of the email chain, especially if it contains any personal data.

- Contact the Data Protection Officer if you are unsure of the best method to send information, particularly personal information.

- Save and file emails and their attachments properly. It is now common business practice for agreements and other business transactions to be done by email. Contractual commitments made by email are as legally binding as hard copy. You should save all business records and documents like contracts, agreements or any other records or connected correspondence, into the relevant file store so that they are managed as corporate records. They may be needed for legal, regulatory, tax, contractual, audit or evidentiary purposes.

- Don't cause offence. Take care that the content or subject matter of any email does not cause offence in any way to a recipient. Email messages must not contain any words, phrases, pictures, or other materials which may be sexually, racially or in any other way abusive or discriminatory, or which may have the effect that a recipient feels that the email is intimidating, hostile or threatening.
- Only retain emails for as long as necessary. Regularly review your email inboxes including sent emails and deleted emails. Familiarise yourself with our retention policy for further information.

Shared (team) email accounts

A 'shared' email account in terms of this procedure is defined as an email account which can be accessed by one or more individuals.

The team must take ownership of the mailbox and ensure that it is managed. Access to mailboxes will only be given as part of the starter process or with direct authorisation from the relevant line manager. Access can be requested or removed by internal IT support.

Requests for a new mailbox are reviewed by the relevant senior manager and an alias email address (an email address that is associated with an already in place destination email address) may be added to an existing team mailbox instead.

Distribution lists and active directory

Distribution lists (DLs) are kept within the office Outlook address book titled 'The Guide Association' and in the excel document named 'region directory'. It is maintained by the PA to the executive and will only contain present staff and region volunteer contact details and group lists.

3) Use of the internet

Girlguiding Anglia provides internet access to support charitable and business activities. Access is granted to Girlguiding Anglia's employees on this basis.

As a user you should:

- Report any suspicious behaviour you see online.
- Only download information if you trust the source and require it to carry out your duties.
- Delete all downloads as soon as you have used or saved them.
- Raise a request with the internal IT support team if you want to install anything from an internet site.

Unsuitable use and unsuitable material

Make sure you understand what is meant by 'unsuitable material'. Unsuitable material includes data, images, audio files or video files which are illegal to transmit under British law; and material that is against the rules, essence, and spirit of this and other Girlguiding and Girlguiding Anglia policies.

It is strictly forbidden to use Girlguiding Anglia digital resources to access the internet at any time for any of the following purposes:

- Carrying out private or freelance business
- Gambling
- Visiting illegal sites
- Conducting personal political activities
- Posting personal views/comments to chat rooms or discussion groups as a staff member (unless specifically authorised in connection with work responsibilities)
- Visiting sites that display materials which could be considered offensive by colleagues. (This could include those that use racist terminology, display nudity or other material of a sexually explicit nature.)
- Download software without prior consent.

Masquerade

You must not masquerade as another employee, ex-employee or volunteer on the internet or post articles in another person's name.

Participation in public internet forums and social media

You are permitted to use work-related internet forums for professional or technical discussion. But you must make every attempt to avoid bringing the name of Girlguiding and/or Girlguiding Anglia into disrepute or adversely affecting its reputation, customer relations or public image.
Non-work-related services – such as social network sites, blogs, chat rooms and bulletin boards – must adhere to the above requirement.

You can find more guidance in section 9 – use of social networking sites.

4) Girlguiding Anglia equipment

As an employee who has had digital equipment issued or loaned to you, you are responsible for its secure storage. It is also your responsibility to make sure any data is stored securely if being carried on portable media or devices.

- You must ensure that any Girlguiding Anglia provided portable devices are kept secure and protected from damage or theft. You must store them in secure locations when not in use or whilst working at home or off site.
- The IT department will use up-to-date anti-virus software (ESET) on all Girlguiding Anglia owned computers or laptops. As employees you must connect your portable device to the network at least once every two weeks to enable the anti-virus software to be updated. This may require you to visit the region office.
- You are also responsible for protecting Girlguiding Anglia's personal information on portable digital devices (like laptops, smartphones, tablets or removable media devices) against physical security threats in accordance with your own personal safety. Note that all Girlguiding Anglia devices will be password & ESET Full Disk Encryption protected as standard.
- As an employee you must not allow your staff login to be used by other individuals - in particular volunteers or individuals who are not Girlguiding Anglia employees.
- You must report immediately any loss of or damage to a Girlguiding Anglia device or personal device which was connected to Girlguiding Anglia systems.
- When leaving a location or travelling with your laptop you must ensure it is shutdown as this ensures the encryption programme works.
- When using any programme or software that allows access to data other than your own, multi factor authentication must be turned on.
- Avoid using your equipment on unsecure public Wi-Fi (ie free Wi-Fi at a conference facility or coffee shop.
- Ensure if you are connecting your equipment to the internet at home that your home Wi-Fi complies with the password guidance from the NCSC.
- You must ensure all equipment is provided for portable appliance testing (PAT) as and when requested.

Removable media devices

The use of removable media devices (for example memory sticks and external hard drives) will only be permitted if there is a valid justification for use. You must demonstrate there are clear business benefits which outweigh the risks. You must never use removable

media devices to store personal information. If you need to use a removable media device, you should contact the data protection officer beforehand for advice.

Cloud services
As users you must only use the cloud services selected, supported, and provisioned by Girlguiding Anglia. Do not use personal storage accounts to store or transfer corporate data. If you have any questions, contact the data protection officer.

Absence from computers
As employees, when you leave your workstation, including at home and in the office, you must lock your computer immediately. Girlguiding Anglia's default setting on laptops and PCs is: if a user does not access their machine for five minutes, then a password-protected screensaver will be applied. Do not override and change this setting.

Security updates
All laptops and desktop computers are automatically set to install both security and application updates. Users are required to fully shut down their machines, ideally nightly, to facilitate these crucial updates.

Bring your own device (BYOD)

- BYOD endpoints accessing Girlguiding Anglia data means more devices that hackers could steal data from. Programmes such as 3CX, Slack and WhatsApp groups contain no data that would compromise the organisation but should only be accessed on personal devices that are password protected (such as a pin code on a mobile phone).
- If you need to access any Microsoft accounts linked to SharePoint/OneDrive (including Outlook), Finance software, HR software or any other programmes that access data other than your own, you must gain permission from the executive manager or data protection officer. This may require mobile device management (MDM) software needing to be uploaded to your personal device.
- If you are using your own device for work related purposes, then you must ensure that your apps are only downloaded from official stores and are on the region's 'safe list'. Please contact the internal IT support team for more information on this if required.

5) Girlguiding Anglia mobile devices

Girlguiding Anglia allows both business and personal mobile phones and tablets etc to connect to the digital systems for work purposes. All mobile phones and tablets connected to Girlguiding Anglia email and cloud services will be subject to a form of mobile device management.

When connected to Girlguiding Anglia systems, you must follow these procedures:

- Security of personal and Girlguiding Anglia owned devices:
    - You must keep mobile phones, laptops and tablets that are connected to Girlguiding Anglia systems secure with a password or pin etc.
    - Apply security measures, such as a lock screen and session timeout.
    - Report a lost or stolen device to the data protection officer immediately:
        - Girlguiding Anglia will ensure access is stopped.
        - You might be charged costs incurred on a Girlguiding Anglia stolen or lost device if you don't report it.
    - Report damage more than normal wear and tear to your line manager immediately.

- Using Girlguiding Anglia owned devices
  These devices are primarily business tools, and you should use them to help with the delivery of Girlguiding Anglia objectives.
    - Where possible, use a Wi-Fi connection when downloading new applications and media.
    - Overseas data roaming can be very expensive. For necessary business data roaming, set your device to use local Wi-Fi connections where possible. Also, set devices to synchronise manually with email and other systems, to ensure costs are managed.

When you leave Girlguiding Anglia you must return all Girlguiding Anglia owned devices to your manager at your exit meeting. You may have financial liability if you do not do this.

Girlguiding Anglia loan equipment

Girlguiding Anglia also provides some items as loan equipment.

- To have these on loan, you need to book through the internal IT support or your line manager. When you sign for the equipment, you will be responsible for its use and for looking after it until you return it.

- Return items to the loan equipment cupboard and ensure you sign them back in and leave them securely.

6) Use of personal and other unauthorised software applications

Only software that has been procured and installed by IT support can be used on Girlguiding Anglia's equipment. This is to ensure that the software is suitable and that the required licences are in place.

If, as a digital user, you need any software over and above what is provided (including for use in a project), you should discuss this with your line manager and IT support who will advise on the suitability, alternatives, cost and feasibility of the products available. You must not attempt to download software, including 'demos', or any other 'free' product from the internet or from any other source, on to any Girlguiding Anglia computer without prior authorisation.

You should be aware that the use of unlicensed software is illegal. In addition, control of the software installed on the Girlguiding Anglia's computer systems is a fundamental requirement to protect the organisation's systems from viruses and other potentially harmful computer programs brought in from outside sources. If you intentionally violate this section of this policy, you will be considered in breach.

7) Password policy

As an employee you must always follow the instructions below:

- Never reveal or share passwords or PINs with another individual, including colleague, line manager or IT support.
- When using the 'remember password' function ensure it is with a secure browser such as Google Chrome or Microsoft Edge and where the account you are using has its own secure password.
- Never write down or store passwords or PINs in paper format, please ensure they are only stored within a password protected document or password protected password manager.
- Always use a strong password (see definition below)

Should you need to share a document containing personal or sensitive information please ensure it is password-protected and the password stored following the password sharing procedure.

Strong passwords

All passwords must:

- Be a minimum of eight characters long
- Include at least three or more of the following:
    - Uppercase character
    - Lowercase character
    - Number
    - Special character

They must not include:

- Any part of the user's username or email address
- Or be the same or like any password used for non-work-related activities

Further advice is available from the National Cyber Security Centre (ncsc.gov.uk).

IT support team responsibilities

IT will ensure the following measures are enforced where direct control is possible in line with our Cyber Essentials accreditation. Any changes, for example due to the functionality of systems or applications, will be documented and the potential risk assessed and reviewed before being implemented.

- User account passwords must be changed every 45 days, all other passwords must be changed if compromised.
- The last ten passwords cannot be re-used.
- An account will 'lock out' following five successive, incorrect log-on attempts.
- Password characters will be hidden by symbols.

On accessing the system for the first time you will need to confirm compliance with the data protection and managing information policy.

All successful and unsuccessful log-on attempts will be logged and may be monitored.

Shared (team) accounts

Girlguiding Anglia shared email accounts will be managed by IT support and linked to existing, personally held Girlguiding Anglia accounts. These accounts will not be able to be accessed directly and no passwords will be assigned.

Where a team has an external shared email or software account the same password policy will apply. In addition:

- This password must not be shared with another individual outside of the authorised users.
- The password must be changed as soon as an individual no longer requires access (including if they leave the team or change role remit).

8) Monitoring

At any time and without prior notice Girlguiding Anglia maintains the right and ability to examine any systems and inspect and review all data recorded in those systems.

All users should be aware that:

- Email usage (including content) may be monitored and recorded centrally
- Internet sites that have been visited can be traced, and Girlguiding Anglia may employ monitoring software to check on the use and content of internet sites accessed
- Any information stored on a computer or device - whether the information is contained on a hard drive, computer disk or in any other manner - may be subject to scrutiny
- An audit or log may be made of files transferred to and from all removable media devices and Girlguiding Anglia owned IT equipment and software may be used to monitor compliance with this policy

Access and monitoring will be necessary, proportionate and carried out with due regard to the rights and freedoms of the employee (for example, their limited but permitted personal use).

Girlguiding Anglia specifically reserves the right for authorised personnel to access, retrieve, read and delete internet access monitoring logs, to assure compliance with this policy.

Where it is suspected that the email and/or internet facilities are being abused by a user, you should contact a senior manager or the executive manager in the first instance.

9) Use of social networking sites

This section of the policy is intended to help staff make appropriate decisions about the use of online social media sites such as blogs, social networking websites, podcasts, forums, message boards, or comments on web-articles, such as Facebook, X (Twitter), LinkedIn, Instagram, TikTok, Pinterest, Tumblr etc, which have become a very significant part of life for many people. They provide a very positive way to keep in touch with friends, colleagues, and our members and can be used to exchange ideas and thoughts on common interests, both personal and work related.

This policy outlines the standards we require staff to observe when using social media and the action we will take in respect of breaches of this policy. If we do become concerned about actions on social media or receive a complaint, we may monitor activity as part of an investigation.

Using social media sites in the name of Girlguiding Anglia and Hautbois Activity Centre.

The communications and opportunities manager, retail manager, Hautbois Activity Centre manager and chief's team will determine who in their team is permitted to post content to social media platforms on behalf of Girlguiding Anglia and Hautbois Activity Centre.

The only exception will be when specific and time limited access is given to another employee or volunteer related to a specific task, project or event. The person allowing access is then responsible for monitoring and supporting the additional person.

Any breach of this restriction will amount to gross misconduct.

We recognise the importance of the internet in shaping public thinking about our organisation and services, employees, partners and customers. We also recognise the importance of our staff joining in and helping shape industry conversation and direction through interaction on social media. The roles listed above are therefore permitted to interact on social media websites about organisational developments. Staff members personal accounts will not be tagged in social media posts to ensure we comply with data protection regulations.

Use of personal social network sites

If an employee's personal internet presence does not make any reference to Girlguiding Anglia or Hautbois Activity Centre and they cannot be identified, then content is unlikely to be of concern. If employment at Girlguiding Anglia or Hautbois Activity Centre is referred to then the information posted would need to comply with the employment conditions outlined below:

a. If an employee wishes to initiate a social networking site or already has one in place, a disclaimer must be used that protects the organisation e.g. 'These are my personal views and not those of Girlguiding Anglia'.

b. An individual is free to talk about Girlguiding Anglia. However, instances where the organisation is brought into disrepute may well be in breach of this policy and will constitute misconduct or gross misconduct and disciplinary action will be applied. Please refer to the disciplinary policy and procedure.

c. An employee should not disclose commercially sensitive, anti-competitive, private or confidential information relating to the organisation, their employment at the organisation or discuss colleagues, staff, competitors, customers or suppliers.

d. Sites should not be used to verbally abuse staff or volunteers. Privacy and feelings of others should be respected at all times. Employees should obtain the permission of individuals before posting contact details or pictures. Care should be taken to avoid using language which could be deemed as offensive to others.

e. Be honest and open but be mindful of the impact your contribution might make to people's perceptions of us as an organisation. If you make a mistake in a contribution, be prompt in admitting and correcting it.

f. You are personally responsible for content you publish onto social media platforms be aware that what you publish will be public for many years.

g. Don't escalate heated discussions, try to be conciliatory, respectful and quote facts to lower the temperature and correct misrepresentations. Never contribute to a discussion if you are angry or upset, return to it later when you can contribute in a calm and rational manner.

h. Always consider others' privacy and avoid discussing topics that may be inflammatory e.g. politics and religion.

i. If information on the site raises a cause for concern regarding a conflict of interest, employees should raise the issue with their line manager.

j. If approached by a media contact about content on a site relating to the organisation, employees should advise their line manager before responding or taking any action.

k. Viewing and updating personal sites should not take place during working hours (non-working breaks excepted).

l. Sites should not be used for accessing or sharing illegal content.

m. Any serious misuse of social networking sites which have a negative impact on Girlguiding Anglia may be regarded as a disciplinary offence.

Use of personal social network sites during working hours

We permit the incidental use of social media websites for personal use subject to certain conditions set out below in section 10. However, this is a privilege and not a right. It must not be abused nor overused, and we reserve the right to withdraw our permission at any time at our entire discretion.

10) Personal use

Limited personal use of Girlguiding Anglia's digital resources is permitted, subject to the restrictions contained in this policy and the other policies. 'Personal use' is defined as any activity that is not work-related or necessary in the performance of duties connected to the employee's employment. You must not request support from other employees or IT support for personal use of digital resources.

Restriction on personal use

The following further restrictions are placed upon all personal use:

- It must be in the user's own time.
- It must be reasonable, appropriate and not excessive.
- It must not interfere with an individual's job responsibilities or those of any other employee.
- It must not adversely impact or disrupt any other digital activity, process or equipment.
- It must not be for the purposes of commercial activity of any kind.
- It must not harm, or be likely to harm, Girlguiding Anglia's reputation.

Liability

No personal use of Girlguiding Anglia's digital property or systems can safely be considered entirely private, and you should not have an expectation of privacy. For example, there should be no expectation of privacy regarding personal emails or internet sites visited including incognito or private browsers.

Girlguiding Anglia accepts no responsibility or liability whatsoever for any loss that you may suffer because of personal use of digital resources.

As a user of Girlguiding Anglia's digital systems for personal use, you do so at your own risk.

In the event of loss or damage to software and/or hardware arising out of personal use, recompense may be sought by Girlguiding Anglia.

Withdrawal of personal use

Personal use of Girlguiding Anglia's resources may be withdrawn at any time and without warning if:

- The use is considered inappropriate by senior managers.
- The use is considered an excessive use by senior managers.
- Any aspect of Girlguiding Anglia's digital equipment, systems or networks are placed at risk.
- The Executive Manager or the Data Protection Officer determine that any restrictions have been breached.
- It constitutes a breach of law.

11) Computer misuse

There is considerable scope for the misuse of computer resources for fraudulent or illegal purposes, for personal interests or for amusement or entertainment.

This section gives you guidelines on what constitutes 'computer resources' and what is considered to be 'misuse'. You should refer to this when you use Girlguiding Anglia's computer resources.

Important - The misuse of Girlguiding Anglia's computer resources is considered to be potential gross misconduct and may mean the individual concerned is liable to disciplinary action, including dismissal.

'Computer resources'

Computer resources include, but are not restricted to, the following:

- Servers (including Cloud servers)
- Desktop computers and laptops
- Tablets
- Smartphones
- Printers
- Network equipment
- Desk phone

'Misuse'

This policy does not define an exhaustive list of all possible forms of misuse of computer resources. Individual circumstances of each case must be considered.

In general, users will:

- Comply with current data protection legislation, supported policies and its associated guidance and will comply with the Computer Misuse Act 1990.
- Not attempt to use computer systems to gain unauthorised access to information and software, or to cause system outages.
- Not deliberately introduce malicious software – such as computer viruses – onto Girlguiding Anglia's network infrastructure and information processing systems.
- Take all reasonable steps to prevent the transmission of viruses by making full use of Girlguiding Anglia's anti-virus software, ensuring it is operating on any device they are using.

Here are some more examples of misuse:

- Use of computer resources for the purposes of fraud, theft or dishonesty.
- Use of computer resources to corrupt, destroy or disrupt the data of other users, or breach their privacy.
- Storing/processing/printing of personal information for a purpose which is not work related.

- Storing/processing of Girlguiding/Girlguiding Anglia's data on personal equipment without prior permission from the executive manager or data protection officer
- Breaching the access control policy, including the password policy.
- Connection of any non-Girlguiding Anglia equipment to Girlguiding Anglia's, in breach of the offsite working policy.
- Unauthorised disposal of digital equipment, for example, destruction, removal or scrapping.
- Theft of, or any parts of any digital equipment.

Administrator rights

Administrator rights will be restricted to a separate username and password, no device should have unlimited local access rights. This ensures control of end-user devices by the external IT company and prevents the accidental download of seemly innocent software that could cause a significant amount of harm or data loss.

12) Other policies

As a user of Girlguiding Anglia IT systems and equipment you must also follow these policies:

- Clear desk and clear screen guidance – cyber security training
- Managing Information policy
- Data breach procedure
  Although the data protection officer will report any data breach they find, you are also responsible for reporting any data breach you find, and you must use the data breach procedure to do this.
- Equality and diversity policy
- All other policies, procedures and guidance required by your role

Further information

Updated: 19/01/2024
Updated to reflect hybrid working: 29/07/2022
Amended to include social media policy: 31/10/2018
Adapted for use by Girlguiding Anglia: 03/07/2018.
Original author: Cathy Fryer, Girlguiding