The Governing and Representative Body of

Arthur Findlay College

PIONEERING SPIRITUALISM
& PSYCHIC SCIENCES

Internet, Communications and Computer Policy

Version Control					
Title:	**Internet, Communications and Computer Policy**				
Author	**Version**	**Date**	**Review**	**Status**	**Comment**
Phil Robinson	ICC001	09.06.2026		Draft	Initial Draft
Phil Robinson	ICC002	03.06.2026		Update	Trusted Regions & Key Contacts
Phil Robinson	IC0003	07.03.2026		Update	Clarification around trusted regions, clarification on monitoring.

Date of Approval	Approved by	Date of next Review	Comments
12-06-2026	NEC	20-06-2026	Approved by majority vote

Contents

Internet, Communications and Computer Policy 3
Purpose: 3
Scope: 3
Key Contacts 3
Relevant legislation and guidance: 3
Acceptable Use: 4
Prohibited Actions: 4
Monitoring 4
Email & Communications: 5
Email Retention: 6
Internet activities: 6
Social Media: 6
AI Use 6
BYOD / Personal Devices & remote working: 7
User Responsibilities: 7
Reporting Security Incidents: 8
Accessibility 8
Further Information: 8

Internet, Communications and Computer Policy

Purpose:

This policy outlines the organisations approach to monitoring, the use of internet, email, computer systems and telephony services. The purpose of this policy is to ensure the safety, security and compliance of all staff, volunteers and the organisation.

Scope:

This policy applies to all employed staff, whether full-time, part-time, contractors, Ministers, Committee Members, volunteers, or any other party working on behalf of or representing The Spiritualists' National Union, Affiliated bodies, or Arthur Findlay College. This policy applies regardless of the geographical location that the individual may be working.

Key Contacts

The following individuals are responsible for overseeing this policy and compliance within the organisation.

Technical Lead | Phil Robinson | 01279 816363 | Phil.Robinson@snu.org.uk

Operations Manager | Steve West | 01279 816363 | Steve.West@snu.org.uk

Relevant legislation and guidance:

Data Protection Act 2018

Computer Misuse Act 1990

Companies Act 2006

Limitation Act 1980

The Privacy and Electronic Communications (EC Directive) Regulations 2003

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation) (Text with EEA relevance)

Acceptable Use:

- All Organisation activities within the individual's role
- Communication with members, churches and the public whilst always ensuring confidentiality and professionalism
- Limited personal use is permitted so long as it does not disrupt work responsibilities, breach company policies or put the organisation at risk

Prohibited Actions:

The following actions fall are categorised as a breach of this policy and could result in disciplinary or legal action taken against the individual.

- The unauthorised installation of 3rd party software on organisational devices
- Downloading or opening suspicious files or files that come from unrecognised senders.
- Unauthorised disclosure of confidential or personal data
- Use of any SNU systems for personal, financial gain and or any unauthorised activities
- Share any passwords, pins or other authentication methods used to access organisational data or systems
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Using the any ICT facilities to bully, harass or promote unlawful activities

Monitoring

Individuals using organisation devices or cloud resources will be subject to appropriate monitoring. This is to ensure the organisation, individual, network, devices are protected. Monitoring is carried to ensure security, compliance and operations of the organisation. Whilst individuals are using organisation assets or accessing organisational data, the individual should keep in mind that any monitoring would be lawful, proportionate and necessary.

Only authorised users may inspect, monitor, filter, record or disclose information in line with relevant legislation and compliance requirements.

Authorised users include

- Members of senior leadership team (limited to the minimum necessary for legitimate organisation purposes)
- Technical Teams including 3rd party partners

Email & Communications:

- All communications must be respectful and professional
- All suspicious emails or phishing emails must be reported (within outlook and or to IT Support)
- Personal data must be only shared where necessary and authorised to do so
- Always protect confidential and personal information
- Report security incidents immediately
- **Users must not** forward chain letters or spam.
- **Users must not** use charity email for political campaigning unless expressly authorised and lawful.

Users must only access their snu.org.uk email accounts from trusted regions unless authorisation is granted on a temporary or permanent basis.

Trusted Regions examples:

- UK
- Europe
- Australia

(If a region is to be permanently granted, then the relevant policies must be updated to reflect, this does not affect any other SNU resources, only snu email accounts.)

Zero Trust policy, all other regions will be deemed as not trusted and users will not be able to access their snu.org.uk emails unless authorisation has been granted.

Some regions we will be unable to allow access even on a temporary basis due to state run monitoring and exploitation, as a result the following countries fall into the extreme high-risk regions;

- China
- Russia
- Iran
- Democratic People's Republic of Korea

Organisational data will be kept for as long as there is an administrative need to keep it to enable the organisation to carry out its business and operations. This will be conducted in line with current legislative and compliance requirements.

Email Retention:

shared / departmental mailboxes will be maintained and retained for the following purposes:

- Business continuity
- Legal obligations (accounts, complaints etc)
- Security & compliance
- Maintaining business records

Exemptions to this will be made on a case-by-case basis but only approved by the organisation's senior leadership team or technical lead.

Internet activities:

- Users must not download copyrighted material
- Users must not access explicit, offensive, discriminative, extremist or any other inappropriate content
- Users must not use peer to peer file sharing unless authorised prior from the Technical Lead
- Users must not use a VPN other than those authorised prior by the Technical Lead
- Users must not attempt to mitigate or circumvent security systems and restrictions
- Users should exercise caution when entering credentials online, if in doubt contact the Technical Lead or your line manager

Social Media:

Please refer to the social media policy found on the SNU website, snu.org.uk

AI Use

- Ensure that no organisational, images, confidential or personal data is entered into any publicly available AI tools.
- Only approved internal AI tools can be used for organisational data that may contain personal data.
- All outputs from AI tools must be reviewed, fact checked for accuracy, copyright, security and compliance

Exceptions:

- Churches committees, members and volunteers may use generative AI for posters, adverts but consent must be obtained if uploading / inputting personal data or images. (written or verbal)

BYOD / Personal Devices & remote working:

We accept that in some circumstances users may use their own device to access organisational data or information, when this is the case, we would ask the following.

User Responsibilities:

Keep the relevant device protected with a strong password, PIN, biometric authentication, or equivalent security measure.

Ensure the device operating system and applications are kept up to date.

Install security updates promptly when available.

Take reasonable precautions to prevent unauthorised access.

Secure the device when unattended.

Report any loss, theft, or compromise of the device immediately.

Users must:

- Access Charity information only through approved systems and applications.
- Avoid downloading or retaining unnecessary Charity information on personal devices.
- Delete Charity information when instructed or when it is no longer required.
- Ensure confidential or personal data is not accessible to family members, friends, or other unauthorised individuals.
- Where possible, Charity information should be stored within approved cloud services rather than directly on personal devices.

Users must not:

- Share Charity information through personal email accounts unless specifically authorised.
- Store sensitive personal data in unsecured locations.
- Disable security controls required by the Charity.
- Allow other individuals to use a device while Charity systems are accessible.
- Use jailbroken, rooted, or otherwise compromised devices to access Charity systems.
- Store confidential or personal information on USB storage devices unless encrypted

Exceptions:

With the above statement "Share Charity information through personal email accounts unless specifically authorised." Individuals, of which set out in the scope may use personal email accounts for charity purposes but only when an organisation email has not been provided.

Reporting Security Incidents:

If an individual notices or suspects a security incident, users must immediately report this to the Technical Lead (Phil.Robinson@snu.org.uk). Where and or if the Technical Lead is unavailable then you must immediately inform your line manager and raise this with the relevant 3rd part providers immediately.

Security incidents may include but not be limited to:

- Lost or stolen corporate devices
- Virus, malware or other intrusive software
- Unauthorised access to a corporate device or data
- Data breaches
- Any security vulnerabilities identified within the organisation infrastructure

Accessibility

The organisation will ensure that any reasonable adjustments are carried out for individuals with disabilities or specific needs so that tasks can be carried out safely and effectively.

These may include but are not limited to:

- Assistive hardware or software
- Alternative security controls where risks have been assessed
- Custom or modified communication formats

Individuals must inform their line manager or contact the technical lead if any accessibility needs are required or if any additional barriers surface. Individuals must only use approved hardware or software which can be granted by the technical lead.

Further Information:

Questions regarding this policy should be directed to one or more of the following:

Technical Lead | Phil Robinson | 01279 816363 | Phil.Robinson@snu.org.uk

Operations Manager | Steve West | 01279 816363 | Steve.West@snu.org.uk

This document will be reviewed annually or in the event of any significant changes to legislation. Should any changes occur or apply to this policy it will be re issued to the organisation.