Information and Communication Technology Policy

Last Update 19/07/2021

Table of Contents

1 Introduction

1.1 The North England Conference (NEC) of Seventh-day Adventists is a non-profit Charity founded upon Christian values.

1.2 Information and Communication Technology (ICT) plays a crucial and transformative role in the work that we do here at the NEC. It is a key component of every activity we undertake and requires proper attention in its own right. Any actions we take must be treated with a caution and duty of care.

At the NEC the structure of the Information Technology function consists of a Head of Technology and external IT support professionals, which is referred to in this policy as Information Technology Support Services (ITS).

1.3 ICT provides unrivalled opportunities to enhance our work practices and activities. At the same time the technology can easily be misused, cause unnecessary risks and liability within and outside of the NEC. The effects could go beyond reputational damage and/or may involve legal implications. Some of the potential dangers but not limited to may be:

- Unauthorised access to or loss or/sharing of personal information;
- The risk of material and immaterial damage through the use of the internet;
- The sharing/distribution of personal images without an individual's consent or knowledge;
- Inappropriate communication/contact with others, including patrons;
- Access to illegal, harmful or inappropriate images and/or other content and/or access to unsuitable internet sites;
- An inability to evaluate the quality, accuracy and relevance of information on the internet;
- Copyright infringement;
- Illegal downloading of content;
- The potential for excessive use of ICT which may impact the NEC and/or individuals within it.

It is essential that the ICT Policy is used in conjunction with any other NEC Policies as set out in the NEC Staff Handbook.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential that this process is well managed and enabled with skills and expertise required to mitigate and/or deal with confidence. The NEC will engage periodically in reminding and/or providing any training required to staff to assist with application of the ICT Policy.

1.4 When using the technology to process or share information it is important that we consider what data we are recording or making available and how this can be viewed or

used by others. Privacy settings should be adjusted when possible to limit the audience who can access this information.

1.5 General Data Protection Regulation (GDPR) was brought in to protect the rights and privacy of individuals and to ensure that data about them was not processed without their consent. It covers personal data held about individuals by the NEC.

2 Policy statement

2.1 The purpose of this policy is to protect all users within the NEC by ensuring that they understand the way in which our organisation's ICT resources are to be used effectively and for their intended purpose.

This policy applies to all members of the NEC community, which may operate for or on behalf of the NEC (including staff, church members, volunteers, patrons) who have access to and/or are users of NEC ICT systems resources, both in and outside of the NEC premises. This policy applies to employees (on any type of Contract) and volunteers.

2.2 The NEC encourages all its employees and volunteers to make effective use of technology, Internet connectivity and internal networks to carry out duties effectively and enhance their work efficiency. Such use should always be lawful and appropriate and should not create unnecessary risk or damage or harm to others. It should not compromise the NEC's information and computer systems nor have the potential to damage its reputation.

2.3 Users are agreeing to all terms and conditions of this policy by logging into, or using, any part of the NEC network infrastructure, and also by using any devices at the NEC office(s) or sites.

3 Scope of the Policy

3.1 The NEC will deal with all incidents within this policy and any other applicable policies by taking required actions to protect the organisation and/or report to appropriate authorities. Where necessary this may mean disciplinary action against employees that breach this policy or supporting policies as set out in the Staff Handbook. Where persons that are not employed by the NEC breach this policy the appropriate action will be taken according to the seriousness of the incident.

4 Roles and Responsibilities

The following section outlines the roles and responsibilities of individuals and groups within the NEC:

4.1 The Officers Committee is responsible for the approval of the policy and for reviewing the effectiveness of the policy.

4.2 The Officers Committee and Head of Technology reviews periodically the information about major incidents and monitoring reports and subsequently makes a report to the EXCOM when required.

- Head of Technology, The Officers Committee and The Human Resources Department are responsible for ensuring that managers and other relevant staff receive suitable training to enable them to carry out their roles to implement the ICT Policy as relevant.

- The Head of Technology will ensure that there is a system in place to allow for monitoring and support of those in NEC who carry out their duties in compliance with the ICT policy.
- The Head of Technology will ensure the Officers Committee and staff are aware of the procedures to be followed in the event of a serious allegation being made against a member of staff and relevant HR/disciplinary procedures.

4.3 The Head of Technology:

- takes day-to-day responsibility for issues and has a leading role in establishing and reviewing the NEC ICT policy and documents;
- ensures that all staff are aware of the procedures to be followed
- liaises and works closely with the external NEC Information Technology Services (ITS) technical staff;
- receives reports incidents and creates a log of incidents to inform of any future developments;
- meets with The Officers Committee to discuss current issues and review incident logs; reports regularly to the EXCOM.

4.4 The Head of Technology is responsible for ensuring:

- that the NEC's technical infrastructure is secure and is not open to misuse or malicious attack;
- that users only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed;
- that they keep up to date with security technical information in order to effectively carry out their role and to inform and update others as relevant;
- that the use of the internal network, internet, remote access, email is regularly monitored and managed in order that any misuse or an attempted misuse can be detected, reported to the appropriate individuals for investigation, action or sanction;
- that monitoring software/systems are implemented and updated in agreement with the NEC policies.

4.5 Staff and Volunteers are responsible for ensuring that:

- they are up to date with the current NEC ICT Policy and practices;
- they report any suspected misuse or problem to the Information Technology Services helpdesk at ithelpdesk@necadventist.org.uk
- all digital communications with staff, volunteers, church members, patrons and members of public should be of a professional level and only carried out using systems managed or accepted by the NEC ITS;
- security issues should be treated with utmost priority in all aspects of the normal working practices and activities;
- assist other employees and help to understand and follow the ICT policy and any related policies;
- they are aware of security issues related to the use devices and that they monitor their use and comply with current NEC policies in regard to these devices.

4.6 Church members and patrons

- are responsible for using the NEC ICT systems in accordance with the Acceptable Use Policy, which they are expected to sign before being given access to the NEC systems;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials

- should understand the importance of adopting good security practice when using digital technologies outside of NEC and realise that the NEC's ICT Policy covers their actions outside of NEC, if related to their activities with the NEC and its lower organisations.

5.1 **Treating Others with Respect**

- The NEC expects everyone to treat Staff and others online with the same standards of consideration and good manners as they would in the course of face-to-face contact.
- Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. The NEC is strongly committed to promoting equal opportunities for all, regardless of race, gender, religious affiliation, cultural background, gender orientation or disability.

5.2 Cyberbullying

- Cyberbullying is a particularly pernicious form of bullying and intimidation, because it can be pervasive and anonymous. There can be no safe haven for the victim, who can be targeted at any time or place.
- Proper supervision of the ICT resources is an important part in creating a safe ICT environment at the NEC;
- Bullying and harassment in any form should always be reported to your line manager in the first instance. Where you consider this to be a conflict in reporting this to your line manager you should report to hrteam@necadventist.org.uk in accordance to the existing policies at the NEC. It is never the victim's fault, and he or she should not be afraid to report the matter.

5.3 Keeping the NEC's Network Safe

- Certain sites may be blocked by the NEC's filtering system and the system may monitor the use of network resources and access. The Head of Technology will oversee the operations of this on a regular basis.
- Email, Internet traffic may be monitored and blocked when treated as SPAM and/or contain certain attachments.
- Staff are issued with their own individual NEC e-mail addresses. Access is using personal login which is password protected. We advise logging off when leaving the computer unattended and keeping all passwords secure.
- Security protection tools are used by the ITS on the networks and devices that connect to it.
- Any member of staff, volunteer or patron who wishes to connect a personal device to the NEC Network will be provided with details on how to do this safely on request.

5.4 Some examples of unauthorised use of the ICT Facilities but no limited to:

- Use of a 3rd-party e-mail service on the NEC network to bypass any monitoring and or restrictions imposed by the organisation
- Use of an unapproved VPN (Virtual Private Network) tools to access any system either within or outside of the organisations IT Network.
- Access to social networking sites via the NEC network during working hours.
- Use the ICT infrastructure for personal commercial or financial gain.
- Interfering with organisations setup, tools, controls and restrictions of the ICT infrastructure in any way.
- Use or attempt to access someone else's account.

- Intentionally seeking offensive material on the Internet. The ICT facilities should not be used at any time to access, download, send, receive, view or display any of the following:
    - Any illegal material.
    - Any message that could constitute bullying, harassment or any negative comment about other persons or organisations.
    - Remarks relating to a person's sexual orientation, radicalisation, gender assignment, religion, disability, age or ethnicity.
    - Online gambling sites.
    - Remarks which may adversely affect the reputation of any organisation or person, whether or not known or believed to be true.
    - Any sexually explicit content.
- All forms of piracy, including the infringement of software licences or other copyright provisions, are illegal. This includes copying, downloading or distributing material from the Internet or e-mail such as computer software, music, text, and video clips. Any content possessed and distributed has to be cleared or permitted by the copyright owner/holder.

5.5 ICT Policy can be found on **NEC&me – WORKSPACE - NEC Policies.** The policy is provided to non-staff requiring access to the NEC's ICT resources. The NEC may impose sanctions for the misuse, or attempted misuse of the internet and other electronic devices.

6. Technical Matters – Infrastructure/Equipment

6.1 The Head of Technology is responsible for ensuring that the NEC's ICT infrastructure and networks are as safe and secure as it is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people and groups named in the above sections will be effective in carrying out their policy responsibilities:

- There will be regular reviews and audits of the safety and security of NEC technical systems;
- Equipment, networks are secured and physical access restricted;
- All users will have clearly defined access rights to NEC ICT systems. Details of access rights available to groups of users will be managed by NEC ITS and will be reviewed annually
- All users will be provided with a username and secure password. Users will be required to change their passwords every six months;
- Users are responsible for the security of their username and password; they must not share it, allow other users to access the system using their log on details and must immediately report any suspicion or evidence that there is a breach of security;
- NEC Information Technology Services staff may monitor and record the activity of users on the NEC ICT systems and users are made aware of this in the Acceptable Use Policy;
- Remote management tools may be used by staff to control, manage devices and monitor user's activity;
- An appropriate system is in place for users to report any actual/potential security incident to the ITS helpdesk (or other relevant person)
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, computers, mobile devices etc. from accidental or malicious attempts which might threaten the security of the NEC systems and data;
- An agreed procedure is in place for the provision of temporary access of "guests" onto the NEC system;
- Only ITS staff are allowed to install software on the NEC computers and devices;

- The use of removable media (e.g. USB drives/CDs/DVDs) by users on NEC computers and portable devices may be controlled, any use should be scanned for viruses before use;
- The NEC infrastructure and individual devices are protected by an up-to-date antivirus software;
- Personal data cannot be sent over the internet or taken off the NEC site unless safely encrypted or otherwise secured.

6.2 Logins and Passwords
Each individual person requiring access to the NEC resources is provided with appropriate access level. Individuals are responsible for ensuring the security of their login details. Under no circumstances login details can be shared or passed on to anybody else. Attempting to access resources using someone's username is prohibited. In accordance with NEC policy, passwords are changed on a regular basis to help ensure that personal information is secure and private.

6.3 Use of Printers
The following rules and guidelines are to be observed:
i) Printing facilities are provided for regular work activities related to organisation. It is not intended for personal use.
ii) Staff must ensure that they do not print excessively or unnecessarily
iii) The NEC may determine printing limits and also control the location and times that printing may be done.

6.4 Installing Hardware and Software
The installation of hardware and software, access to the network is a sole responsibility of ITS. Staff are forbidden to install any software without consulting with the ITS first. Hardware installation or relocation can only happen with the approval from ITS. Failure to follow the above requirements may result in a breach of law and may lead to the disciplinary process in line with this policy.

6.5 Bring Your Own Device (BYOD)
The NEC accepts that third party devices may be used to access organisation's resources. However, there are a number of security considerations for such scenarios. Use of BYOD should not introduce vulnerabilities into existing secure environments and users should refer to the Acceptable Use Policy. The following provides a brief overview of the key points:

- The NEC has a set of clear expectations and responsibilities for all users;
- The NEC adheres to the General Data Protection Regulation (GDPR) principles;
- All users are provided with and accept the Acceptable Use Policy;
- All network systems are secure and access levels for users is differentiated;
- Where possible these devices will be covered by the NEC's management systems
- All users will use their username and password and keep them safe;
- Regular audits and monitoring may be conducted to ensure compliance;
- Any device used for access to the NEC ICT resources should be reported immediately to ITS helpdesk for loss, theft, change of ownership.

7. Telephone/Communications

7.1 In normal circumstances, staff should not share any personal contact details with non-employees and this includes personal mobile telephone numbers, home telephone numbers, online identities and accounts. Personal email addresses, online identities or accounts, for use in conducting work are prohibited.

7.2 When using communication technologies, the NEC considers the following as good practice:

- The official NEC email service may be regarded as secure and monitored;
- Users should be aware that email and phone communications may be monitored;
- Users must immediately report, to the nominated person, in accordance with the NEC policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening and must not respond to any such communication;
- Any communication between Staff and outside the office must be professional in tone and content. This applies to any form of communications not limited to verbal or written. These communications may only happen using official and approved by the NEC channels. Personal email addresses, text messaging or social media must not be used for these communications;
- Personal information should not be posted on the NEC website and only official email addresses will be used to identify members of staff.

7.3 Spamming is forbidden.

7.4 Posting Anonymous Messages and forwarding Chain Letters is forbidden. Chain letters commonly contain viruses, misleading information or hoax threats

7.5 Email resources are limited and as such should not be used in a manner that results in unnecessary overload or inconvenience.

8. Data Protection

8.1 Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (GDPR). The GDPR sets out seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

These principles should lie at the heart of your approach to processing personal data. Confidentiality and data protection policies will apply and should be consulted for details.

8.2 Staff must ensure that they:

- At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse;
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data;
- Transfer data using encryption and secure password protected devices.

8.3 When personal data is stored on any portable device, USB drive or any other removable media:

- the data must be encrypted and password protected;
- the device must be password protected
- the device must offer approved virus and malware protection;

- the data must be securely deleted from the device, in line with NEC policy once it has been transferred or its use is complete.

9. Social Media – Protecting Professional Identity

9.1 The NEC, who is the responsible body a duty of care to provide a safe environment staff and volunteers. The NEC could be held responsible for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the NEC liable to the affected party. Reasonable steps to prevent any harm must be taken.

9.2 The NEC, who is the responsible body will provide the following measures to ensure reasonable steps are in place to minimise risk of harm:

- through limiting access to personal information:
- Clear reporting guidance, including responsibilities, procedures and sanctions;
- Risk assessment, including legal risk.
- Training

9.3 NEC staff should ensure that:

- No reference should be made in social media to any individual staff, church member, or member of public
- They do not engage in online discussion on personal matters relating to members of the NEC community;
- Personal opinions should remain personal and should not be attributed to the NEC;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

9.4 The NEC's use of social media for work purposes may be checked and monitored regularly for safeguarding and reputational purposes.

9.5 Social Media policy continues to apply and should be consulted for more details.

10. **Discipline Guidance**

Anything suspicious or a breach of this policy and supporting policies as set out in the Staff Handbook needs to be reported to the Head of Technology and recorded by the persons reporting the issue. Persons should state date, time and a summary of the issue. Any incident will be treated as a disciplinary matter and appropriate people need to be informed.
Major, repeated, flagrant or habitual incidents will be treated as a serious disciplinary issue. Actions/response will be proportionate to the severity of the incident and may result in a dismissal from the duties and/or employment.

<u>Remote Working</u>

At the NEC, there may be circumstances whereby staff are required to work remotely on a temporary basis. To work remote also includes home-working. Where this occurs all Remote workers agree:

- To be bound by the terms of this policy, ensuring care & compliance at all times;
- The proper use, care, maintenance and safekeeping of information assets & allocated device(s);

- To ensure that they follow the process detailed in the policy in the event that a device is lost or stolen;
- To ensure the appropriate use of devices whilst carrying out NEC work;
- To ensure that passwords are not stored with the device.
- To ensure that data gathered throughout the course of your work for the NEC is backed up onto the NEC systems and network. Failure to backup data to corporate systems will result in unrecoverable data loss if the device storage fails. Failure to comply with this policy will be investigated and might lead to disciplinary action being taken.

11. Conclusion

ICT allows us to communicate with others, both in and outside the Organisation. Our aim is to promote the positive use of the technology and to discourage inappropriate usage or usage which could put the NEC and any person at risk. Staff are asked to recognise that this policy is designed to protect the interests of the individuals with work with and for, to guide staff and to ensure that appropriate actions are taken at all times. The policy subject to be reviewed periodically and as required. Any changes or updates to the current version will be communicated and provided.