

# National Navigation Award Scheme (NNAS)

## Cybersecurity Policy

Version	Date	Author	Type
V1	19/01/2024	Jane Howie	First Draft
V1.1	23/01/2024	Pete Hawkins	Review and edits
V1.1	11/04/2025	M Handford	Final Version signed off

### 1. INTRODUCTION

The purpose of this policy is to highlight the potential risks of cyberattacks to the NNAS, making clear what we currently have in place to prevent such events occurring, and to highlight what is regarded as the basic principles of good cyber security.

A cyber-attack is an attack launched from one or more computers against another computer or network of computers. It can maliciously deactivate computers, steal data, or use a compromised computer as a launch point to further aggravate the attack. The two aims of cyber-attacks are to either disable the system or gain illegal access to the target computer or network.

In the past few years, the National Cyber Security Centre (NCSC) has issued a number of alerts to charities, warning of an increase of malware attacks targeting charitable institutions.

The complexity and variety of cyberattacks is ever increasing. While cybersecurity prevention measures differ for each type of attack, good security practices and basic IT hygiene are generally good at mitigating these attacks.

In addition to implementing good cybersecurity practices, we are advised to keep systems and security software up to date, enable firewalls and threat management tools and solutions, install antivirus software across systems, control access and user privileges, backup systems often, and proactively watch for breached systems.

### 2. SCOPE OF THE POLICY

This policy covers all employees, consultants, Trustees, and volunteers. All individuals are required to understand and comply with the terms of this policy.

The policy and guidelines apply to all electronic media and services that are:

- accessed on or from the NNAS' premises.
- accessed using the NNAS' computer equipment, either in the office or at home.
- accessed from an individual's own devices, (when accessing NNAS services), either remotely or by wireless within the premises, and / or used in a manner that identifies the individual with the NNAS.

Any deliberate breach of the policy may result in disciplinary action up to and including dismissal with immediate effect for gross misconduct. In addition, the NNAS may, if it considers it appropriate, report a breach of this policy and procedure to the relevant authorities.

It is acknowledged that threat actors are constantly learning new ways to deceive people into succumbing to phishing. Therefore, everyone is encouraged to speak up or notify leadership in the event of a breach or suspected breach. No blame will be assigned for accidental errors.

## National Navigation Award Scheme (NNAS) Cybersecurity Policy

Prompt notification of such incidents will facilitate a faster response, limit damage, and contribute to improved education for all.

### 3. RESPONSIBILITIES UNDER THE POLICY

Managing ICT and Cyber security are important aspects of strategic leadership within the NNAS, as such the Trustees have a responsibility to:

- Ensure that the policy is effectively communicated and consistently applied.
- Ensure that mechanisms are in place to ensure that all relevant individuals are aware of this policy.

The Admin Manager has a responsibility to:

- Ensure that staff understand what is expected of them within the policy and guidelines.
- Monitor staff to ensure compliance with this document.
- Notify the Chair of any concerns arising under this policy, including related concerns about security breaches or misuse.
- Ensure that networks and devices are managed and administered in such a way that they comply with this policy.

### 4. CHANGES TO POLICY

This policy does not form part of a Contract of Employment with NNAS, and NNAS reserves the right to make additions or alterations to the policy from time to time and, when this happens, you will be notified of any such changes.

### 5. COMMON TYPES OF CYBERATTACKS

The most common types of cyber-attack methods used by cybercriminal gangs around the world:

#### Phishing

Phishing is a technique used to deceive a target into taking harmful action such as downloading malware disguised as an important document. A targeted phishing attack could be used to gain access to a user's account that has important information (such as a member of the Board of Trustees) or a user with administrative privileges to the network.

Phishing is usually in the form of an email sent to either a list of users or targeted at single user. The attacker would craft an email and disguise it to be seemingly normal, with malware attached that looks like it could be a normal document. The email could also include a link that goes to a website designed to look like a familiar website and trick the user into entering their credentials.

To prevent phishing attacks, it is recommended the email system should have an effective filter, implementing email authentication methods like SPF, DKIM, DMARC and MTA-STS to filter potential spam. Users should also be trained on how to identify potential spam emails before clicking on any links or documents attached.

#### Ransomware

## National Navigation Award Scheme (NNAS)

### Cybersecurity Policy

Ransomware encrypts important files on the system so the user cannot access them. The attacker then demands payment to restore access to the files.

The attacker may also threaten to release sensitive documents (medical, financial, disciplinary) to the internet unless a ransom is paid.

A ransomware attack usually happens when a user opens a malware file or link on a network connected computer. The malware file has specific scripts to identify and encrypt important files. Ransomware could be used to encrypt financial and contact data so that the NNAS would not be able to access it.

To prevent ransomware attacks, it is a good practice to have On-access scanning enabled on all user devices to scan for viruses before accessing files. Firewalls should be enabled on host devices and anti-virus software should be updated with the latest security patches.

All files critical for the continued functioning of the NNAS should be regularly backed up and an external copy of the backup should be kept to ensure it cannot be encrypted.

#### **Password attack**

Password attack is an attempt to gain access to systems by cracking the user's password. Once the user password is cracked, the attacker can gain access to either confidential data or an administrative account allowing access to all data or make significant changes to the network.

A targeted password attack usually involves the attacker finding out details about the user and then attempting to use that information to determine the correct password. A good practice to follow is not using the same password twice.

The use of complex passwords of appropriate length with a mixture of words, numbers, and special characters is strongly advised by cybersecurity experts. Use of two factor authentication will also help guard against this type of attack. Adoption of Passkeys as a preferred method of logging in, as and when they are available.

#### **Brute force**

Brute force is an attempt to gain access to systems by trying different passwords to eventually guess the correct one. Similar to a password attack, the attacker could gain access to privileged user accounts.

Malware that is installed on the network with direct access to a systems login screen can be used to secretly attempt to guess a user's password.

One of the prevention tactics is to set a maximum number of login attempts. Accounts should lockout if there are too many failed attempts at logging in. Audit logs should also be configured and regularly reviewed by the system administrator for any abnormal use of accounts.

#### **Denial of Service (DDoS)**

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding

## National Navigation Award Scheme (NNAS) Cybersecurity Policy

infrastructure with a flood of Internet traffic. An attacker compromises a computer or multiple computers using malware that instructs them to send traffic to a single target.

Systems should be built and configured around the concept of redundancy and the ability to fail-over to a secondary system if the first is unavailable. Systems should also be designed with the ability to deal with increased load over the average normal usage.

### 6. ANTI-CYBERATTACK MEASURES

Measures taken by NNAS to mitigate the above risks:

#### **Network security**

The NNAS computers have their Firewalls enabled. Wifi is protected by a strong password which has been changed from the default setting. Guest wifi is separate to the NNAS Office wifi.

#### **Email**

The NNAS uses Google Workspace for its email system. Email is encrypted using Transport Layer Security (TLS). This is a protocol that securely encrypts and delivers inbound and outbound mail while disabling eavesdropping between mail servers. Most major email providers use TLS but it is important to keep in mind that both the sender and receiver must use a TLS supported mail server to encrypt messages.

#### **Backup**

The NNAS backs up critical files in the Cloud, specifically Google Workspace. In addition, external back up of critical files are regularly undertaken and stored in a locked office cabinet.

#### **Anti-Virus**

NNAS computers are protected by Malwarebytes Antivirus. This scans the computer for threats daily. It also scans USB drives when they are connected to the computer. Malwarebytes Browser Guard blocks access to websites which contain malware and viruses.

#### **Passwords**

NNAS has a Password Policy that gives users guidance on how to create and store strong passwords.

### 7. PRIVACY AND MONITORING

Those using the electronic communication services should be aware that there is no legitimate expectation of privacy in the use of these services and individuals should consider alternative means of communication for highly sensitive or confidential information. The NNAS reserves the right, at the discretion of the Chair of the Board of Trustees, to review any electronic files and messages held on any computer or other device and to review an individual's usage of any electronic media, services, system or device to the extent necessary to ensure that electronic media, services, systems or devices are being used in compliance with the law and with this and the NNAS' other policies. This can involve the reading of business and personal email contents and attachments to verify the validity of the content. A similar process is

## National Navigation Award Scheme (NNAS) Cybersecurity Policy

undertaken to assess and categorise web pages and web mail. This will always be done in accordance with the law.

### 8. DATA PROTECTION

The NNAS is fully committed to compliance with the 2018 General Data Protection Regulation. In order to protect the privacy of employees, Trustees, course Providers and candidates, these rules must be followed by staff, Trustees and volunteers:

- Any data transferred to or from the NNAS should be stored on an encrypted USB stick with an appropriately secure password.
- When emailing secure information staff should compress the data within an encrypted RAR or ZIP file using an appropriately secure password.
- Staff should report any data breaches or concerns to the Admin Manager
- Staff shall comply with the data retention timelines outlined in the Privacy Policy.

**Any queries regarding this document should be addressed to the Admin Manager at [info@nnas.org.uk](mailto:info@nnas.org.uk)**