Cyber Security Policy

Safeguarding is Everyone's Responsibility

Date: 29 January 2026 , Updated June 26

Next Review: January 2027

Definitions

- **Software** includes operating systems, commercial off-the-shelf applications, extensions, interpreters, scripts, libraries, network software and firewall and router firmware.
- **Devices** includes all types of hosts, networking equipment, servers, networks, and end user devices such as desktop computers, laptop computers, thin clients, tablets and smartphones — whether physical or virtual.
- **Organisational data** includes any electronic data belonging to our organisation, for example, emails, documents, database data, financial data.
- **Organisational service** includes any software applications, cloud applications, cloud services, user interactive desktops and mobile device management (MDM) solutions that our organisation owns or subscribes to. For example: web applications, Microsoft 365, Google Workspace, mobile device management containers, Virtual Desktop solutions or IP telephony.
- **A sub-set** is part of the organisation whose network is segregated from the rest of the organisation by a firewall or VLAN.
- **Servers** are devices that provide organisational data or services to other devices as part of our organisation's business.
- **Vulnerability fixes** include patches, updates, registry fixes, configuration changes, scripts or any other mechanism approved by the vendor to fix a known vulnerability.
- **Licensed and supported software** is software that we have a legal right to use and that a vendor has committed to support by providing regular vulnerability fixes. The vendor must provide the future date when they will stop providing these. (Note that the vendor

doesn't need to have created the software originally, but they must be able to now modify the original software to create fixes).

- **Passwordless authentication** is an authentication method that uses a factor other than user knowledge to establish identity. Examples include but are not limited to; biometric data, physical devices, onetime codes, QR codes, and push notifications.

Scope Boundary & Overview

This policy refers to the Cyber Security of the whole IT infrastructure owned and managed by Next Steps Education Ltd, not limited to:

All devices and software in scope and which meet any of these conditions:

- can accept incoming network connections from untrusted internet-connected hosts
- can establish user-initiated outbound connections to devices via the internet
- control the flow of data between any of the above devices and the internet

Asset Management

The device assets within this scope include:

- Four HP desktop computers currently running Windows 11 (2x HP 24-cb1002na 23.8" All-in-One PC, 1x HP All In One PC 23" CR0, 1x 1x HP All In One PC 27" CR0)
- One HP Laptop currently running Windows 11 imminent (HP 20C21)
- One HP Deskjet 4100C Printer
- One HP Officejet Pro 9720e

Cloud Assets

Our organisation accesses a number of SaaS based assets which are included within this scope include:

- Microsoft 365 Cloud Subscription for Business, monthly subscription
- TutorCruncher cloud software platform, monthly subscription
- Quickfile secure accounting platform, yearly subscription
- Hubspot secure content and marketing platform
- TutorOnboarder cloud software platform, monthly subscription
- Bright HR cloud software platform, yearly contract

Within these assets, controls are implemented as follows:

- FIREWALLS – the Cloud provider
- SECURE CONFIGURATION – both our organisation and the Cloud provider
- SECURITY UPDATE MANAGEMENT – the Cloud provider
- USER ACCESS CONTROL – our organisation
- MALWARE PROTECTION – the Cloud provider

All accounts our organisation owns are in scope, even when those accounts are used by a third party, such as a supplier, contractor or Managed Service Provider (MSP) to manage or support our infrastructure.

BYOD & Remote/ Home Working

BYOD is included in this scope.

Protections

Firewalls

All devices have configured software firewall, and our organisation has:

- changed default administrative passwords to a strong and unique password and disabled remote administrative access entirely
- prevented access to the administrative interface (used to manage firewall configuration) from the internet, unless there is a clear and documented business need, and the interface is protected by multi-factor authentication
- blocked unauthenticated inbound connections by default
- ensured inbound firewall rules are approved and documented by an authorised person, and include the business need in the documentation
- removed or disabled unnecessary firewall rules, when they are no longer needed
    - Devices are not used on unprotected, public wifi

Secure Configuration

Our organisation proactively manages our computers and network devices, regularly:

- removing and disabling unnecessary user accounts (such as guest accounts and administrative accounts that won't be used)
- changing any default or guessable account passwords
- removing or disabling unnecessary software (including applications, system utilities and network services)
- disabling any auto-run feature which allows file execution without user authorisation (such as when they are downloaded)
- ensuring users are authenticated before allowing them access to organisational data or services
- ensuring appropriate device locking controls for users that are physically present

Security Update Management

Our organisation recognises that any device that runs software can contain security flaws, known as vulnerabilities. To mitigate risk, we make sure that all software in scope is kept up to date, ensuring all software on in-scope devices must:

    - be licensed and supported
    - removed from devices when it becomes unsupported or removed from scope by using a defined sub-set that prevents all traffic to / from the internet
    - have automatic updates enabled where possible
- be updated, including vulnerability fixes, within 14 days* of release, where:
    - the update fixes vulnerabilities described by the vendor as 'critical' or 'high risk'
    - the update addresses vulnerabilities with a CVSS v3 base score of 7 or above
    - there are no details of the level of vulnerabilities the update fixes provided by the vendor

User Access Control

We recognise that every active user account in our organisation facilitates access to devices and applications, and to sensitive business information. By making sure that only authorised individuals have user accounts, and that they're only granted as much access as they need to carry out their role, we reduce the risk of information being stolen or damaged. Accounts with special access privileges have enhanced access to devices, applications and information. If these accounts are compromised, an attacker could take advantage of their greater accesses to corrupt information on a large scale, disrupt business processes or gain unauthorised access to other devices in the organisation. Our organisation retains control of our user accounts and the access privileges that allow access to our organisational data and services.

This means we:

- have in place a process to create and approve user accounts
- authenticate users with unique credentials before granting access to applications or devices
- remove or disable user accounts when they're no longer required
- implement MFA, where available – authentication to cloud services must always use MFA
- use separate accounts to perform administrative activities only (no emailing, web browsing or other standard user activities that may expose administrative privileges to avoidable risks)
- remove or disable special access privileges when no longer required (when a member of staff changes role, for example)

Password-based authentication

All user accounts require the user to authenticate. Where this is carried out using a password, we have put in place the following protective measures:

- Protecting passwords against brute-force password guessing by implementing multi-factor authentication
- Using technical controls to manage the quality of passwords, including

- using multi-factor authentication
- A minimum password length of at least 8 characters, with no maximum length restrictions and use automatic blocking of common passwords using a deny list.
- Supporting users to choose unique passwords for their work accounts by:
  - educating people about avoiding common passwords, such as a pet's name, common keyboard patterns or passwords they have used elsewhere. This could include teaching people to use the password generator feature built into some password managers.
  - encouraging people to choose longer passwords by promoting the use of multiple words (a minimum of three) to create a password (such as the NCSC's guidance on using three random words)
  - providing usable secure storage for passwords (for example a password manager or secure locked cabinet) with clear information about how and when it can be used.
  - not enforcing regular password expiry o not enforcing password complexity requirements

Should a password or account be compromised, we have an established process in place to change passwords promptly.

Multi-factor authentication (MFA)

As well as providing an extra layer of security for passwords that aren't protected by the other technical controls, we always use multi-factor authentication to give our administrative accounts extra security, and accounts that are accessible from the internet. The password element of the multi-factor authentication approach must have a password length of at least 8 characters, with no maximum length restrictions. We also use an additional factor of an authentication app on a trusted device, or in some cases SMS.

Passwordless authentication

Passwordless authentication is a method of verifying identity without using traditional passwords. Where it is available, we encourage the use of passwordless authentication including:

- Biometric authentication
- One-time codes
- Push notifications

Malware Protection

Our organisation recognises risks arising from malware, such as computer viruses, worms and ransomware, including potential sources such as; malicious email attachments, downloads (including those from application stores), and direct installation of unauthorised software.

Our organisation uses in-built anti-malware and malware screening configured to:

• be updated in line with vendor recommendations

• prevent malware from running

• prevent the execution of malicious code

• prevent connections to malicious websites over the internet.

Backing Up Our Data

Our organisation recognises the risks from cyber- attack and stores a back-up of all data held by the organisation, which is renewed weekly.

BYOD (Bring Your Own Device)

We recognise that by allowing remote access to our organisation by devices that we do not control (non-organisation-owned computers and phones) we increase the risk of material being used by someone for purposes we may not authorise or agree. Company or sensitive information could be copied, modified, transferred to our competitors or just made public.

A further risk is that the owner of the computer may install apps from insecure sources, perhaps not even realising the risks, and this could make our organisation's files vulnerable to attacks from malware. Failing to update a device can also leave it open to security threats.

Our employees, contractors and clients who own the computer may leave their device lying around unsecured (after all, they are probably working from home). They may allow friends and family to use it. Other issues include controlling the content and access of a private device if a user leaves our company or sells their device and erasing our organisational information if the device is lost or stolen.

To mitigate the risks of BYOD, we insist that any devices that are used to access our company data, systems and platforms comply with the following:

- The Operating System and apps must be fully supported by the manufacturer and receive security updates
- Software based firewalls are activated and configured correctly. Security updates must be installed within 14 days
- Cyber Essentials password controls are applied to users' own devices (BYODs)
- Users logging in on computers and tablets have a day-to-day account, and this is separate to the administrator account
- The device automatically locks when not in use and requires a 6 digit or more pin/pass code to unlock, (use a biometric if available)
- Anti-malware software is installed on devices and kept updated or, for a mobile device, only apps from the manufacture's respective store are allowed to be installed
- Unused apps should be uninstalled
- If lost or stolen, it must be reported to the business promptly
- Rooting or jailbreaking is not permitted

Furthermore, we operate our SaaS and networks with zero trust architecture wherever possible, elevating our security and minimising our risk to cyber-attack.

Cloud Assets

Cloud assets and SaaS within our business are protected by 2MFA where available. Decisions on new software applications are made in regard to its own cyber security and 2MFA operation.