NORTHAMPTON SCHOOL FOR GIRLS

Respect for Self | Respect for Others | Respect for Learning

Cyber Security Policy

Author:	AFY
Approval Date:	12 November 2025
Approval Body:	Finance, Risk & Audit Committee
Review Date:	November 2026
Version:	V1

Version	Date	Updates
V1	**November 2025**	New policy

Associated Policies	• Data Protection • Online Safety and Acceptable Use Policy • Use of Artificial Intelligence (AI) • Filtering and Monitoring Procedures

1	**Policy Statement of Aims**
1.1	Cyber Security has been identified as a risk for Northampton School for Girls (NSG) and everyone needs to contribute to ensure data security. We have invested in technical cyber security measures, but we also need our employees to be vigilant and act to protect the IT systems.
1.2	The Headteacher is responsible for cyber security at NSG.
1.3	Employees may be subject to disciplinary action if they breach this policy.
2.	**Purpose and Scope**
2.1	The purpose of this document is to confirm the systems and controls that are in place to protect NSG from cyber criminals and associated cyber security risks.
2.2	This policy is relevant to all staff and trustees.
3.	**Types of Threats**
3.1	**Cybercriminals and Cybercrime**
	Cybercriminals are generally working for financial gain. Most commonly, for the purposes of fraud; either selling illegally gained information to a third party or using it directly for criminal means. Key tools and methods used by cybercriminals include: • **Malware**: malicious software that includes viruses, Trojans, worms or any code or content that could have an adverse impact on organisations or individuals • **Ransomware:** a kind of malware that locks victims out of their data or systems and only allows access once money is paid • **Phishing:** emails purporting to come from a public agency to extract sensitive information from members of the public.
3.2	**Hacktivism**
	Hacktivists will generally take over public websites or social media accounts to raise the profile or a particular cause. When targeted against local government or school websites and networks, these attacks can cause reputational damage. If online services are regularly disrupted by cyber-attacks, this could lead to the erosion of public confidence in using such services. Hacktivist groups have successfully used distributed denial of service attacks to disrupt the websites of several councils already.
3.3	**Insiders**
	Staff may intentionally or unintentionally release sensitive information or data into the public domain. This may be for the purpose of sabotage or to sell to another party, but more often than not is due to simple human error or a lack of awareness about the particular risks involved.
3.4	**Zero-day threats**
	A zero-day exploit is a cyber attack that occurs on the same day a weakness is discovered in software. At that point, it's exploited before a fix becomes available. It is an attack that exploits a previously unknown security vulnerability. This poses a risk to any computer or system that has not had the relevant patch applied, or updated its antivirus software.
3.5	**Physical threats**
	The increasing reliance on digital services brings with it an increased vulnerability in the event of a fire, flood, power cut or other disaster, natural or otherwise, that impacts upon our IT systems.
4.	**Potential Consequences**
4.1	The following are all potential consequences of cybercrime; • Financial cost • Breach of confidentiality and data protection

	• Regulatory breach • Reputational Damage • Business Interruption • Structural and Financial Instability
5.	**Prevention**
5.1	Given the seriousness of the consequences noted above, it is important for NSG to take preventative measures and for all staff to follow the guidance within this policy.
5.2	NSG have put in place a number of systems and controls to mitigate the risk of falling victim to cybercrime. These include technological solutions as well as controls and guidance for staff.

5.3	The following data and cybersecurity steps are taken and also shared in our Online Safety and Acceptable Use Policy:
	• Use strong passwords (password complexity is enforced); periodic updates, and account security.
	• Keep software, firewalls, antivirus, and security features up to date; systems will be periodically reviewed to address evolving cyber threats.
	• Follow the school's BYOD policy when using personal devices; authorisation from the Headteacher is required to access or transport school data on personal devices or USBs.
	• Store all personal data securely, in line with GDPR and the school's Data Protection Policy
	• Use encryption where appropriate to protect sensitive information
	• Log out of systems, lock devices when unattended, and shut down at the end of each day to prevent unauthorised access.
	• Not attempt to access systems or files without permission, all access rights are assigned and reviewed by the Network Manager. Any accidental access or misdirected information must be reported immediately to the IT team
	• Not download, store, or transport student or staff data on unauthorised external storage devices
	• Provide regular staff training, including phishing identification, email safety, and cybersecurity awareness. Training will cover how to check email sender addresses, verify requests for bank details or payment changes, and respond to suspicious messages. This training will also be included in staff induction.
	• Ensure staff are aware of how to report cybersecurity incidents, including whom to contact (e.g., DSL, Network Manager, Data Protection Officer) and the required procedures.
	• Require the mandatory use of VPN and Multi-Factor Authentication (MFA/2FA) for remote access, critical system access, and school-provided services including email and cloud storage.
	• Prohibit the use of unauthorised external storage devices (e.g., USB drives) and personal cloud storage platforms for school data.
	• Conduct third-party cybersecurity audits (e.g., 360 Safe) annually to test the effectiveness of controls.
	• Maintain a layered approach to cybersecurity:
	  ○ Ensure all systems are kept up to date, with software updates and security patches applied promptly.
	  ○ Maintain an active and enabled firewall.
	  ○ Conduct regular access and permissions reviews to ensure staff have the appropriate level of access.

	• Automatically back up critical data daily, including online backups with an air gap and local backups to dedicated backup servers (e.g., at 10 p.m. each evening). • Delegate responsibility for management information system (MIS) security to a third party provider, supported by the Network Manager. • Assess the security of suppliers and contractors, including verification of Cyber Essentials certification where appropriate. • Develop, review, and test the incident response plan with the IT team every six months or after any significant incident, using the NCSC's 'Exercise in a Box' tool to simulate and improve real-world response readiness. • Never engage with ransom requests in the event of a ransomware attack, as this does not guarantee recovery of data.
5.4	All students and staff sign Acceptable Use Agreements before accessing school systems.
6.	**Cybersecurity Risks for Girls**
6.1	As a school that is a single-sex community for girls aged 11-16, we are aware of the unfortunate growing risks that young girls are facing in the digital world. In Laura Bates' book, *"The New Age of Sexism: How the AI Revolution is Reinventing Misogyny*", she warns that online platforms and algorithms are evolving and often replicate and amplify existing gender biases.
6.2	This results in new threats, in the form of deepfakes, image-based abuse and grooming tactics. Young girls are particularly vulnerable because AI tools can be exploited to generate realistic fake images or manipulate social media content.
6.3	We want to ensure that our students have a strong cybersecurity education and digital literacy to empower them to protect their online identities, recognise manipulation and have the courage to advocate for accountability in shaping their digital environments.
7.	**Training**
7.1	All staff and trustees undertake annual cyber security training, supported by the National Cyber Security Centre and a certificate is issued upon completion.
8.	**Policy Review**
8.1	This policy will be monitored as part of the annual internal review or as required by legislative changes.

Appendix 1: Exams

1.	Purpose
1.1	This document details the measures taken at NSG to mitigate the risks of cyber threats.
1.2	The Headteacher recognises the need for staff involved in the management, administration and conducting of examinations to play a critical role in maintaining and improving cyber security at NSG.
1.3	In addition to adhering to industry best practices, the following areas are addressed in this document to ensure that members of the exams team protect their individual digital assets: • Creating strong unique passwords • Keeping all account details secret • Enabling additional security settings wherever possible • Updating any passwords that may have been exposed • Setting up secure account recovery options • Reviewing and managing connected applications • Staying alert for all types of social engineering/phishing attempts • Monitoring accounts and reviewing account access regularly
2.	**Roles and Responsibilities**
2.1	The **Head of Centre** will ensure that members of the exams team, led by the IT team, adhere to best practices in relation to the management of individual accounts and centre wide cyber security (detailed at Clause 5.3 of policy).
2.2	**The Exams Officer** will ensure: • Best practice is followed in relation to the management of individual accounts • Evidence is provided of an awareness in relation to cyber security (annual training) • Training is undertaken on the importance of creating strong unique passwords and keeping all account details secret and on all types of social engineering/phishing attempts
3.	**Complying with JCQ Regulations**
3.1	The Head of Centre ensures that there are procedures in place to maintain the security of user accounts in line with JCQ regulations (sections 3.20 and 3.21 of the *General Regulations for Approved Centres document)* by: • providing training for authorised staff on the importance of creating strong unique passwords and keeping all account details secret • providing training for staff on awareness of all types of social engineering/phishing attempts • enabling additional security settings wherever possible • updating any passwords that may have been exposed • setting up secure account recovery options • reviewing and managing connected applications • monitoring accounts and regularly reviewing account access, including removing access when no longer required • ensuring authorised members of staff securely access awarding bodies' online systems in line with awarding body regulations regarding cyber security and the JCQ document *Guidance for centres on cyber security*: www.jcq.org.uk/exams-office/general-regulations • Authorised staff will have access, where necessary, to a device which complies with awarding bodies' multi-factor authentication (MFA) requirements. • reporting any actual or suspected compromise of an awarding body's online systems immediately to the relevant awarding body

4.	Cyber Security Best Practice
4.1	The Head of Centre ensures that all staff involved in the management, administration and conducting of examinations/assessments at NSG stay informed about the latest security threats and trends in account security.
4.2	All staff and trustees undertake annual cyber security training, supported by the National Cyber Security Centre and a certificate is issued upon completion. Records of cyber security training are retained for all staff and are available for inspection.
4.3	By adopting industry standard cyber security best practices, the Head of Centre is significantly reducing the risk of cyber-attacks and protecting valuable data and assets within the centre.
4.4	If a cyber-attack which impacts any learner data, assessment records or learner work is experienced, the Exams Officer will contact the relevant awarding body/bodies immediately for advice and support.
5.	**Account Management Best Practice**
5.1	All staff take the steps as stated in Clause 5.3 of this policy to ensure data and cybersecurity measures are in place on all systems.