General Data Protection Regulation (GDPR)

Nottingham Schools Trust Acceptable Use Policy

May 2018

Acceptable Use Policy

Contents

Acceptable Use Policy.

1. Introduction

Nottingham Schools Trust (NST) Acceptable Use Policy does not aim to impose unreasonable restrictions. The NST is committed to protecting its employees, partners and itself from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, Internet browsing and FTP are the property of the NST. These systems are to be used for business purposes in serving the interests of the NST in the course of the NST's normal operations.

Ensuring effective security of the NST's network is a joint effort involving the participation and support of every NST employee and any associated colleagues who deal with NST information and/or information systems. It is the responsibility of every computer user to be aware of these guidelines and to comply with them.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at the NST. These rules are in place to protect both employees and the NST itself. Inappropriate use exposes the NST to unacceptable risks including virus attacks, compromised network systems and possible legal challenge.

3. Scope

This policy applies to the use of information, electronic and computing devices and network resources to conduct NST business, or interact with internal networks and business systems, whether owned or leased by the NST, an NST employee or a third party working on behalf of NST (such as Trustees, SIA's, External Consultants). All employees, contractors, consultants, temporary and other partners working on behalf of NST are responsible for exercising good judgment in relation to appropriate use of information, electronic devices and network resources in accordance with NST policies and processes as well as the law and relevant codes of practice.

This policy applies to Trustees, employees, contractors, consultants, temporary and all other partners or workers working on behalf of NST, including personnel affiliated to third parties.
Use of "Employees" below, shall be taken to mean Trustees, employees, contractors, consultants, temporary and other partners or personnel working on behalf of NST or affiliated to third parties.

4. Policy

General Use and Ownership

NST's CEO is responsible for the operation of the policy. The policy covers NST information stored on electronic and computing devices whether owned or leased by NST, an employee or a third party and remains the sole property of the NST. You must ensure through legal or technical means that information is protected in accordance with current data protection legislation.

Employees and all others accessing the NST's computing resources have a responsibility to promptly report the theft, loss or unauthorised disclosure of NST proprietary information.

Employees and all others may access, use or share NST proprietary information only to the extent it is authorised and necessary to fulfil their assigned job duties.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. The NST is responsible for creating specific guidance concerning personal use of Internet/Intranet/Extranet systems. In the absence of such guidance, employees should refer to the NST's general policies or guidance on personal use of NST resources. Where there is any uncertainty, employees should consult their supervisor or manager.

For the purpose of maintaining security and integrity of the network, authorised individuals within NST may monitor equipment, systems and network traffic at any time.

The NST reserves the right to audit its networks and systems on a periodic basis to ensure compliance with this policy.

Security and Protected Information

All mobile and computing devices that connect to the NST's internal network must comply with the minimum standards set by the NST / SchoolsIT.

System level and user level passwords must comply with the NST's password policy/criteria. Providing access to another individual, either deliberately or through failure to secure the network access, is prohibited.

All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. Users must lock the screen or log off when the device is unattended for a reasonable amount of time. When working offsite i.e. outside NST's offices, users must lock the screen or log off whenever the device is unattended.

If an NST employee posts messages from an NST email address to newsgroups, etc. they must include a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the NST, unless posting is in the course of business duties.

Employees must use extreme caution when opening e-mail attachments received from unknown senders as they may contain malware.

5. Unacceptable Use

The following activities are generally prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of the NST authorised to engage in any activity that is illegal under local bye laws, national law or international law while using NST-owned or leased resources.

The lists below are not exhaustive, but try to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities.

The following activities are strictly prohibited, with no exceptions:

- Damage to the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of copied or other software products that are not appropriately licensed for use by NST.
- Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music and the installation of any copyrighted software for which NST or the end user does not have an active license is prohibited.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

- Using NST computing assets to actively engage in procuring or transmitting material that is in violation of harassment and/or other workplace regulations.
- Making fraudulent offers of products, items or services originating from any NST account.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network snooping, pinged floods, packet spoofing, denial of service and forged routing information for malicious purposes.
- Executing any form of network monitoring which will intercept data not intended for the employee's host account, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host network or account.
- Interfering with or denying service to any user, for example, denial of service attack.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, NST employees to parties outside the NST.

Email and Communication Activities.

When using NST resources to access and use the Internet, users must appreciate that they represent the NST. The following activities are strictly prohibited, with no exceptions:

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email or telephone, whether through message frequency or size of messages.
- Unauthorised use or forging of email header information.
- Creating or forwarding "chain letters".
- Use of unsolicited email originating from within NST 's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the NST or connected via NST 's network.

- Posting the same or similar non-business-related messages to large numbers of newsgroups (newsgroup spam).

Blogging and Social Media

- Blogging use of social media by employees, whether using the NST ’s resources and systems or personal computer systems is also subject to the terms and restrictions set in this policy. Limited and occasional use of the NST’s systems to engage in blogging and social media is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate the NST’s policy, is not detrimental to the NST’s best interests and does not interfere with an employee's regular work duties. Blogging and use of social media from the NST’s systems is also subject to monitoring.
- The NST’s approach towards confidential information also applies to blogging and social media. As such, employees are prohibited from revealing any of the NST’s confidential or protected information, or any other material considered to be confidential by the NST when engaged in blogging or accessing social media.
- Employees shall not engage in any blogging or use of social media that may harm or damage the reputation and/or goodwill of NST and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by NST’s policy around non-discrimination and anti-harassment.
- Employees may also not attribute personal statements, opinions or beliefs to the NST when engaged in blogging or social media. If an employee is expressing his or her beliefs and/or opinions, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the NST. Employees assume all risk associated with blogging use of social media.
- Apart from following all laws applying to the handling and disclosure of copyrighted materials, the NST’s trademarks, logos and any other NST intellectual property may also not be used in connection with any blogging or social media activity.

6. Policy compliance measurement

The NST’s CEO will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits and feedback from employees.

7. Exceptions

Any exception to the policy must be approved and recorded by the NST's CEO.

8. Non-compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

9. Related policies and processes

- Data Protection Policy
- Email Policy

10. Review

This policy will be reviewed annually.

V1.0 May 2018