Use of IT Resources, Security of Information and Cyber Security Policy

Policy Name	Use of IT Resources, Security of Information & Cyber Security Policy
Policy Number	NYSF Policy 7.0
Effective Date	1 April 2019
Date Last Reviewed	April 2020
Scheduled Review Date	March 2021
Responsible Person	CEO

Policy

Purpose

This policy and procedures outline the National Youth Science Forum's (NYSF's) guidelines and provisions for using and preserving the security of IT resources, data, and technology infrastructure.

The NYSF relies on technology to collect, store and manage information, and in doing so is vulnerable to security breaches. Human errors, hacker attacks and system malfunctions could cause significant organisational damage and may jeopardize the NYSF's reputation.

NYSF employees, contractors and volunteers are required to use IT resources during their engagement with the NYSF. This policy and procedures inform users of their obligations when using NYSF IT resources.

Scope

This policy and procedures apply to all NYSF employees, contractors, volunteers and anyone who has permanent or temporary access to NYSF systems, information, and IT resources, including remote or travelling employees.

Use of IT Resources

1. The NYSF provides Information Technology (IT) and communication facilities to enable the effective conduct of its business.

2. The moderate use of telephones, computers, email and the internet for personal use by employees is acceptable; however, personal use must be kept to a minimum during work hours.
3. Employees may use the email system to send non-business-related emails; however, personal use is regarded to be a privilege and must be used appropriately. Employees should be aware that they should not send emails that contain material that may be considered to be offensive or inappropriate to others or damaging to the NYSF.
4. Use of internet access must be moderate, and employees must not access inappropriate sites such as pornographic, gambling sites or sites containing offensive material. The NYSF has the right to access individual usage to check if private use is inappropriate or excessive.
5. Where an employee fails to comply with reasonable and appropriate email and internet access requirements, their conduct may be investigated in line with the NYSF Code of Conduct Policy and may result in dismissal.
6. Use of personal devices such as mobile phones in the office is acceptable, subject to moderate use and employees acting with consideration for their co-workers when using devices.
7. The NYSF uses social media such as Facebook, Instagram and LinkedIn to promote its programs. Employees must not use social media forums to comment negatively or inappropriately about matters relating to the NYSF, or concerning its employees, business partners, volunteers or program participants, both past and present.

Security of Information

8. Consistent with the NYSF's Privacy Policy, the NYSF will only use and disclose personal information for the purpose it was provided for and will take reasonable steps to protect private or sensitive information from misuse, interference and loss, as well as unauthorised access, modification or disclosure.
9. Confidentiality of information is paramount, and employees must undertake practices which ensure the safe storage of personal information and confidential data. Lockable storage cabinets must be used to store private and confidential information securely. This includes information about program participants, employee information, financial information, and intellectual property of the NYSF.
10. NYSF employees must act with respect when handling participant personal information and confidential data and be mindful of not leaving personal information or confidential data readily accessible (either on computer screens or in hard copy documents) to other people who do not have a legitimate need to know about it. Employees must also take extra care if using work-related personal information outside of the office, such as working from home or attending meetings. Where personal information is used outside of the office, it should be appropriately stored, or if on an electronic device, access should be limited to the NYSF employee only.

Cyber Security

11. The use of personal and company devices, including desktop computers, laptops, and mobile phones, introduces a security risk to the NYSF’s data. Employees are required to keep their personal and company-issues devices secure, both physically and digitally.
12. NYSF employees use email to communicate with each other, with stakeholders, and with the wider public, and are expected to do so safely and professionally.
13. NYSF employees access many password-protected accounts in the course of their employment, and employees are expected to create and maintain the security of access to these accounts. This is achieved by using password management software to generate and store passwords (e.g. Dashlane),

enabling two-factor authentication where available, limiting the sharing of accounts and passwords, and where sharing of a password is necessary, sharing it through a secure channel.

14. Working outside of the NYSF Office presents additional cyber security risks, as the NYSF is less able to control the security of NYSF devices and data. Employees who are working remotely, including during work travel, are obliged to follow this policy and the associated procedures during their time outside of the office, and comply by the additional procedures outlined in the section *Working Remotely*.
15. Backups of NYSF's information are performed regularly and stored securely., both on physical external hard drives and on the cloud.
16. On ending employment with NYSF, all employee's accounts are closed or made inactive
17. NYSF students, partners, stakeholders, and employees should feel that their data is safe. All members of the NYSF community should contribute to ensuring the safety and security of NYSF's information by being vigilant and prioritising cyber security.

Procedure

Use of Email

1. Managers should ensure that employees understand expectations around using email in terms of moderate personal use and clearly understand what constitutes inappropriate use.
2. Employees should be made aware that personal emails must not contain material that amounts to gossip about colleagues or that could be offensive, demeaning, persistently irritating, threatening, discriminatory, involves the harassment of others or concerns personal relationships.
3. No material is to be sent as a defamatory email, in breach of copyright or business confidentiality, or prejudicial to the good standing of the NYSF in the community or to its relationship its employees, business partners, volunteers or program participants and any other person or business with whom it has a relationship.
4. If a manager has concerns about an employee's personal use of email, they should speak to the Manager, Corporate Services to gain access to information to check if an employee's usage is excessive or inappropriate.
5. Employees should be aware of the risk of scams and malicious software being transmitted via email, and take the following steps to avoid virus infection or data theft:
    a. Avoid opening attachments or clicking on links when the content of the attachment or link is not adequately explained or expected (e.g. "watch this video, it's so funny!").
    b. Be suspicious of emails with clickbait subject lines or content (e.g. offering prizes or giveaways).
    c. Check the names and email addresses of senders to ensure they are legitimate (e.g. nysf@bigpond.com vs nysf@nysf.edu.au).
    d. Look for inconsistencies in email content (e.g. poor English from a native English speaker, requests to reply to/from different email addresses, emails received at unusual times/days or when the sender is on leave/unavailable, requests for information irrelevant to the sender's role).
    e. Verify any unusual or unexpected requests with the sender in person or by phone to ensure they are the genuine sender. Emails requesting payments, changes of bank details, or login information are particularly important to verify.

6. If an employee isn't sure that an email they have received is safe, they should refer it to their Manager or the Manager, Corporate Services, and not respond to the email.

Use of the Internet

7. Managers should ensure that employees understand expectations around internet usage in terms of moderate personal use and clearly understand what constitutes inappropriate use.
8. Appropriate personal use might include accessing the internet to do internet banking, check the weather forecast or make a booking or appointment online. Managers should talk to staff about the boundaries of acceptable use to ensure they clearly understand expectations. For example, it may be regarded as inappropriate for an employee to check Facebook continuously all day or spend long periods browsing general interest sites.
9. Employees should be made aware that their browsing history can be checked for content and duration. If a manager has concerns about an employee's personal use of the internet, they should speak to the Manager, Corporate Services to gain access to information to check if an employee's usage is excessive or inappropriate.

Professional Use of Social Media

10. The NYSF expects its employees to maintain a certain standard of behaviour when using Social Media for work or personal purposes.
11. NYSF maintains many social media platforms. The release of all social media content under the NYSF name and brand is managed by the External Relations team, as part of their program of work. Members of other NYSF teams may from time to time be asked to contribute or support this work.
12. All content using any NYSF-related name, hashtags, images, logos, or associated content, must be cleared by the Manager, External Relations or their delegate.
13. Any team member who is asked to support social media engagement should access the NYSF platform as facilitated by the External Relations team, not by posting from their personal social media accounts. This policy does not preclude the sharing of NYSF-related or issued social media content via personal accounts.
14. Employees must ensure that they have approval is to engage in Social Media as a representative or on behalf of the NYSF and that any social media related work that they engage in is conducted professionally at all times and in the best interests of NYSF.
15. Employees must be mindful not to release any confidential information or material that violates the privacy or publicity rights of another party on social media relating to NYSF or its employees, business, partners, volunteers program participants, both past and present, and program applicants.

Private Use of Social Media

16. NYSF acknowledges its employees, contractors and sub-contractors have the right to contribute content to public communications on websites, blogs and business or social networking sites not operated by NYSF. However, inappropriate behaviour on such sites has the potential to cause damage to NYSF as well as its employees, business partners, volunteers or program participants.
17. Therefore, employees must also refrain from posting, sending, forwarding or using, in any way, any inappropriate material including but not limited to material which could cause insult, offence, intimidation or humiliation to NYSF or its employees, business partners, volunteers or program participants; or is defamatory or contains confidential information concerning stakeholders.

Security of Information

18. Managers should ensure that employees are aware of the requirements to securely maintain and store sensitive and confidential information within the workplace. This includes the establishment of systems and protocols for saving and filing confidential emails and personal information on the NYSF's IT system.
19. Employees must be careful in the handling of hard copy confidential information and ensure that student application or medical information is not left unsecured on desks when not being used. Also, only those employees with a need-to-know should access such information. All confidential documents should be stored in lockable filing cabinets, which are locked when not being accessed
20. Employees should seek permission from their manager to remove sensitive information from the office either electronically or on hard copy.
21. Employees, including Board Members, should not share, disclose, or discuss confidential or sensitive information via non-secure channels, such as webinar platforms, including during internal meetings being held through such platforms. Rather, such information should be distributed securely via Dropbox to those with authorised access and referred to in meeting proceedings.
22. Inattention to adhering to these protocols may be regarded as a performance/conduct issue.
23. All files about the NYSF should be stored in the appropriate location on the NYSF Dropbox account. Any files not stored on the NYSF Dropbox account are at higher risk of being irreversibly lost should NYSF infrastructure fail or be compromised.
24. Files should be shared via Dropbox rather than via email to ensure that access to the file is restricted to the intended recipient.

Use of Devices

25. Employees should keep all devices password-protected, including personal devices which contain or are used to access NYSF information.
26. Employees should ensure that they do not leave their devices exposed or unattended in insecure environments and should ensure devices are locked and password protected when leaving them unattended in secure environments such as the NYSF Office or home.
27. Employees are advised to avoid accessing NYSF systems and accounts from other people's devices or lending their own devices to others.

Password Management and Account Access

28. NYSF employees are issued with a Dashlane password management account which should be used to generate and store all passwords used to access NYSF accounts or information.
29. Employees should use Dashlane's *Password Health Score* tool to assess the security of their accounts and improve their password security to ensure their score remains over 80.
30. Where it is not possible to use a Dashlane-generated password, a password with at least eight characters, including capital and lowercase letters, numbers, and symbols should be chosen. Chosen passwords should not contain easily guessed information, such as names, birthdays, or common numerical sequences (e.g. 123 or 111).
31. An employee's Dashlane account must also be secured using a password which meets the above requirements.
32. Passwords for accounts which are accessed by multiple employees should be shared using Dashlane's sharing functionality, rather than being shared via email, text message, post-it note etc.

33. If passwords must be shared outside of Dashlane, they should be exchanged in-person where possible, or via a phone call, where they can verify the identity of the recipient.
34. Where available, two-factor or multi-factor authentication should be enabled.

Working Remotely

35. When working remotely, employees should continue to follow all policy and procedural items included in this document.
36. Employees should not access NYSF systems or information using public Wi-Fi networks.
37. Employees should ensure that their home Wi-Fi network is password protected prior to accessing it on an NYSF device.
38. When working in a public or shared space, employees should be conscious of their surroundings and avoid working on or discussing sensitive information if it may be visible to or overheard by the public.
39. Prior to period of increased levels of working remotely, it should be ensured that full backups of the NYSF Dropbox account are conducted and appropriately stored, as per the below section *Backups*.

Reporting Security Breaches

40. The NYSF Management and Corporate Services Teams need to know about scams, breaches (both attempted and successful) and suspicious activity so they can better protect NYSF infrastructure.
41. Staff are required to report perceived attacks, suspicious emails, phishing attempts, and any other activity that they consider suspicious or risky, to their Manager.
42. Managers are required to forward any reports to the Manager, Corporate Services, who must investigate promptly and resolve the issue.
43. Where staff are aware of security breaches committed by or affecting another staff member, they are encouraged to confidentially report this to their Manager for further investigation and resolution.
44. Any major breach of cyber security, where NYSF information or data has been accessed or is at high risk of being accessed, must be reported to the NYSF Board by the CEO.

Backups

45. The Corporate Services Team should conduct a full backup of the NYSF Dropbox account quarterly. This backup should be stored offsite on an external hard drive which is accessible only to the Manager, Corporate Services, and CEO.
46. If NYSF Employees choose to store files outside of Dropbox, or in their private Dropbox folder, they are responsible for backing up these files.