IT Usage Policy Template

Updated 28th May 2020

**Contents**

Aim of this Policy 3

Use of Network Accounts 3

Related Documents 3

Passwords 3

Security of Computers, Laptops and other electronic devises 3

Unacceptable behavior 3

Organisation-owned information held on third-party websites 4

Monitoring 4

Failure to comply 4

Agreement 4

Review 4

Appendix One – Password policy 5

# Aim of this Policy

Use of email and the internet by employees of (name of your organisation)is permitted and encouraged where such use supports the goals and objectives of the organisation.

Employees, contractors, and volunteers must ensure that they:

* comply with current legislation.
* use email and the internet in an acceptable way.
* do not create an unnecessary business risk to (name of your organisation)through their misuse of email and the internet.

# Use of Network Accounts

All individually allocated usernames, passwords, and email addresses are for the exclusive use of the individual to whom they are allocated. Each employee and volunteer are personally responsible and accountable for all activities carried out under their username.

* Use of a network account implies and is conditional upon acceptance of this policy.
* No one may use, or attempt to use, IT resources allocated to another person, except when explicitly authorised by the provider of those resources.
* Individuals are personally responsible for all activity carried out under their user name, and must not share their password with any other person (except where it is requested by IT Support to assist them in support activity).

# Related Documents

See also Data Protection Policy for background on personal data handling.

# Passwords

Unless specifically agreed in writing, individual passwords should not be divulged to anyone else (other than the System Administrator) and will be regularly changed (at least annually). It is appreciated that some systems have a general password for (name of your organisation); these should be kept secure and not used by any unauthorised person. All passwords are to be reset when a possible breach is detected and the Systems Admin needs to be informed of the breach.

Full details of the password policy are given in [Appendix One](#_Appendix_One_–) of this document.

# Security of Computers, Laptops and other electronic devices

When using computers, laptops and network enabled devices, employees must:

* Log off their computer or device at the end of the working day or whenever the computer or device is left unattended.
* Portable devices present a particular risk to data, and workers are responsible for ensuring that all data they store on any laptop is secured, whether or not the device is permanently allocated to them.
* Take care not to view sensitive data in any location where the screen might be visible to members of the public or other organisations.

# Unacceptable behaviour

In particular, the following is deemed unacceptable use or behaviour by employees:

* Sending email and visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material
* Using the computer to perpetrate any form of fraud, or software, film or music piracy
* Using the email to send offensive or harassing material to other users
* Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or another such license
* Hacking into unauthorised areas
* Publishing defamatory and/or knowingly false material about (name of your organisation), your colleagues and/or our customers on social networking sites, ‘blogs’ (online journals), ‘wikis’ andany online publishing format
* Revealing confidential information about (name of your organisation)in a personal online posting, upload or transmission - including financial information and information relating to our customers, business plans, policies, staff and/or internal discussions
* Undertaking deliberate activities that waste staff effort or networked resources
* Introducing any form of malicious software into the corporate network.

# Social Media

Guidance for all Staff using social media for business

This policy should be read alongside the data protection and acceptable use policies, which are particularly relevant to staff using social media.

Users must not:

* Create or transmit material that might be defamatory or incur liability.
* Post messages, status updates or links to material or content that is inappropriate.
* Inappropriate content includes pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism or materials relating to cults, gambling, or illegal drugs.
* This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone on the basis of race, age, sex, religious or political belief, national origin, disability, sexual orientation or any other characteristic protected by law.
* Use social media for any illegal or criminal activities.
* Send offensive or harassing material to others via social media.
* Broadcast unsolicited views on social, political, religious, or other non-business-related matters.
* Use social media for advertising or endorsement purposes.
* Send or post messages or material that could damage (name of your organisation)’s image or reputation.
* Discuss colleagues, customers or suppliers without their approval.
* Post, upload, forward or link spam, junk email, chain emails and messages.

# Organisation-owned information held on third-party websites

If you produce, collect and/or process business-related information in the course of your work, the information remains the property of (name of your organisation). This includes such information stored on third-party websites such as webmail service providers and social networking sites, such as Facebook and Twitter.

# Monitoring

(name of your organisation)accepts that the use of email and the internet is a valuable business tool. However, misuse of this facility can have a negative impact on employee productivity and the reputation of the organisation.

In addition, all of the (name of your organisation)email and the internet-related resources are provided for business purposes. Therefore, (name of your organisation)maintains the right to monitor the volume of email and the internet and network traffic, together with the email and the internet sites visited. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

# Failure to comply

Where it is believed that an employee has failed to comply with this policy, they will face the (name of your organisation)disciplinary procedures laid out in the Grievance and Disciplinary Policy. If the employee is found to have breached this policy, they will face the disciplinary process, the actual penalty applied will depend on factors such as the seriousness of the breach along with the employee's disciplinary record.

# Agreement

All (name of your organisation)employees, volunteers or Trustees who have been granted the right to use the organisation's email and the internet access are required to confirm understanding and acceptance of the terms and conditions of this policy.

**Transfer of data**

Where sensitive data (e.g. that which may make it possible to identify clients, users or staff) is transferred to or from clients, care needs to be taken to ensure that the (name of your organisation)policies on data protection are fully complied with. If there are any concerns regarding the security of such data transfers then processes need to be put in place to password protect such data. No data is to be transferred outside of the GDPR regulations introduced in May 2018.

For details of the Data Protection requirements see separate policy.

Data transfer should as a rule not be without password protection or restricted access and by preferance should be via hosted SharePoint sites. No data should be transferred without the knowledge of the Data Lead in (name of your organisation).

# Review

These procedures will be reviewed by the (name of your organisation)Board of Trustees every five years, after consultation with employees or to accommodate alterations to current legislation, reforms or Employment Law.

# Appendix One – Password policy

Password Policy

## **Overview**

Computer user accounts grant access to (name of your organisation)Information Systems. The process of creating, controlling, and monitoring user accounts is extremely important to an overall security program.

## **II. Purpose**

Identification and authentication access controls play an important role in helping to protect Information Systems. The purpose of this policy is to protect Information Systems by defining requirements for new passwords and changes to passwords.

## **III. Scope**

This policy applies to all (name of your organisation) staff that utilise Information Systems with IDs and passwords (credentials). This policy applies whether staff are using (name of your organisation)Information Systems, staff owned devices for organisation approved work, or staff use Information Systems of third party service providers for work related activities.

## **IV. Policy**

The Manager with responsibility for IT systems and support shall ensure:

* Policies and procedures manage the process of creating, changing, and safeguarding passwords/phrases.
* Policies and procedures prevent staff from sharing passwords/phrases with others.
* Procedures advise staff to commit their passwords/phrases to memory and not to be written down.
* Policies and procedures govern the password/phrase change frequency.

This Policy applies to all (name of your organisation)related authentication activities including, but not limited to, the following:

* Administrator accounts.
* User accounts.
* Network infrastructure devices (e.g. firewalls, routers, wireless access points, etc.).
* Third party service providers.
* Web applications.
* Mobile devices.

## **A. New User Accounts**

When granting access for a new user/account:

* System administrators will establish a unique ID and unique password/phrase.
* The user password will be provided to the user in a secure manner.
* When the user logs on for the first time, the user will be required to change their initial password/phrase to something that meets the requirements of this policy.

## **B. Selecting Passwords/Phrases**

Phrases are not the same as passwords. A phrase is a longer version of a password and is typically composed of multiple words. The phrase “We're off to see the wizard, The Wonderful Wizard of Oz” could be converted to WotstwTWWoO as an example. By converting some letters to numbers or special characters, the phrase is even more secure.

When selecting a new password/phase, system administrators and users must select passwords/phrases that are long, strong, and complex. Where possible, Staff shall choose passwords/phrases that meet the following requirements:

* Contain both upper and lower case characters (e.g., a-z, A-Z).
* Include both numbers (0-9) and special characters (e.g. @, #, $, \*).
* Have a minimum of at least 10 characters and preferably 15 characters long and is a phrase.
* Where possible, use different passwords/phrases for general office activities (e.g. e-mail, file access) vs. systems that store sensitive or confidential data.

Staff should not choose passwords/phrases that:

* Include common words such as those found in a dictionary.
* Are the same as passwords/phrases used on Staff personal accounts (e.g. personal e-mail, on-line banking, or social media).
* Contain personal information such as a spouse or pet’s name, national insurance number, street address, phone number, etc.
* Contain sequences or repeated characters. For example, 1234, 3333, etc.

Staff with special system privileges, assigned by a transaction, program, process, or group membership, should select a unique password/phrase from other accounts held by that individual.

## **C. Password/Phrase Guidelines**

Staff shall follow security guidelines to ensure passwords/phrases are not compromised. Training and awareness programs shall ensure Staff is:

* Educated on security related risks.
* Reminded of security requirements when selecting and protecting passwords/phrases.
* Educated not to select the "Remember Me" or “Remember Password” feature in web applications and browsers.
* Reminded to be careful when using social media so the password/phrase is not compromised.

Passwords/phrases must not be:

* Revealed to anyone.
* Stored, written down, or transmitted in clear (unencrypted) text.
* Inserted into unencrypted e-mail messages or other forms of electronic communications.

If a Staff member believes that their password/phrase has been compromised or made available to others, the Staff member must immediately change their password and notify IT Staff.

If someone demands a password, refer them to this policy or have them contact the IT Department.

## **D. Password/Phrase Changes**

Passwords/phrases must be changed on a regular basis according to the following schedule:

* All administrator passwords/phrases must be changed at least once every 12 months.
* All user passwords/phrases must be changed at least once every 12 months.

## When selecting a new password/phrase, Staff shall not repeat any of their prior Three passwords/phrases.

## **E. Software Applications**

Application developers must ensure programs contain the following security precautions:

## **Applications** must require each user to have their own unique ID where reasonable (e.g. not shared, no user groups).

* Passwords/phrases and Sensitive Information must be protected using strong encryption.
* Passwords/phrases and Sensitive Information must not be transmitted or stored in clear text.
* Ensure applications timeout and require the user to enter a password/phrase after a period of inactivity.

## **V. Enforcement**

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

## **VI. Distribution**

This policy is to be distributed to all staff and volunteers with access to (name of your organisation) Information Resources.