Title: Information Technology Policy
Section: Organisational

Written by: Kelly Reaburn
Contributors: Ian Jager

Policy Statement

UBC relies on technology to perform day to day function of the Club.

Purpose and Scope

This Policy clarifies staff, member, volunteers and committee usage and conditions relating to UBC IT Infrastructure and work devices, including mobile phones, laptop, computers and storage devices.

This policy sets out the standards of behaviour expected of staff, members, volunteers and committee using UBC's internet, email and computer facilities, or when making reference to UBC on external sites.

This Policy applies to working outside normal working hours, are working off-site, and during work related functions.

This policy applies to all people who use UBC's computer network by any means (users). The policy also applies to users who contribute to external blogs and sites that identify themselves as associated with UBC.

Definitions

UBC: The Uncle Bobs Club

"Blogging" means the act of using a web log or 'blog'. 'Blog' is an abbreviated version of 'weblog' which is a term used to describe websites that maintain an ongoing chronicle of information. A blog is a frequently updated website featuring diary-style commentary, audio-visual material and links to articles on other websites.

"Confidential Information" includes, but is not limited to trade secrets of UBC, non-public information about the business and affairs of UBC such as: marketing or strategy plans; exclusive supply agreements or arrangements; commercial and business plans; contractual arrangements with third parties; financial information and data; technical data; proposals and intentions; designs; policies and procedures documents; concepts not reduced to material form; information which is personal information for the purposes of privacy law; and all other information obtained from or obtained in the course of working or providing services to UBC that is by its nature confidential.

"Computer Surveillance" means surveillance by means of software or other equipment that monitors or records information input or output, or other use, of UBC's computer network (including, but not limited to, the sending and receipt of emails and the accessing of websites).

"Computer Network" includes all internet, email and computer facilities which are used by users, inside and outside working hours, in the workplace of UBC or at any other place while performing work for UBC. It includes, but is not limited to, laptop computers, tablets and other handheld electronic devices, smart phones and similar products, and any other means of accessing UBC's email, internet and computer facilities, including, but not limited to, a personal home computer which has access to UBC IT systems.

"Intellectual Property" means all forms of intellectual property rights throughout the world including copyright, patent, design, trade mark, trade name, and all confidential information and including know-how and trade secrets.

"Person" includes any natural person, company, partnership, association, trust, business, or other organisation or entity of any description and a Person's legal personal representative(s), successors, assigns or substitutes.

Policy

GENERAL ITEMS

Users need to abide by the following general items:

- Users are responsible for protecting their username/password and any information used and/or stored on/in their UBC account.
- UBC accounts are to be used for company related activity and are not to be used for non-related activities.
- Users are required to report any weaknesses in the computer security and incidents of possible misuse or violation of this agreement.
- Users are not permitted to access any data or programs contained on UBC systems for which they do not have authorisation or explicit consent of the owner of the data/program.
- Users shall not make unauthorised copies of copyrighted software, except as permitted by law or by the owner of the copyright.
- Users shall not purposely engage in activity with the intent to harass other users, degrade the performance of the systems, allow an unauthorised user access; obtain extra resources beyond those allocated; circumvent UBC's computer security measures or gain access to a UBC's system where authorisation has not been given.

<u>Downloading files and applications</u>

There is a high risk involved in downloading files, programs and content from the internet. This can subject your computer to a virus and can compromise the integrity of the entire IT infrastructure. Please check first if unsure when downloading internet material.

<u>Information security</u>

Basic security requirements are put in place to which you need to be aware and must comply. These include:

- Passwords must not be written down
- Physical access to servers and network equipment including hubs and routers is to be restricted to authorised personnel only
- After 10 minutes of inactivity a password-protected screen saver will be enforced
- On cessation of employment of a staff member, State Committee shall terminate all access privileges for the employee
- Yearly backup of all data is stored centrally. Monthly backups are retained in the cloud for disaster recovery purposes in accordance with backup procedures
- The use of portable storage devices such as USB's / Hard drives is prohibited without authorisation from State Committee.

Internet Usage

Internet access is an essential tool in a modern workplace. UBC's internet facility has been provided to assist staff in the performance of their day to day business related duties. The intent of the following guidelines is to clarify the responsibilities of staff use of the internet and to establish professional and ethical conduct of good internet usage.

Unacceptable Usage

The internet must not be used to:

- Defame, harass, abuse or otherwise offend other internet users, individuals, or organisations.
- Knowingly download, store or distribute offensive material (eg. pictures and literature) or contrary to law material containing defamatory comments.
- Attempt to obscure the origin of any message or download material under the assumed internet address or otherwise disguise user identity.
- Knowingly obtain unauthorised access to information or damage, delete, insert or otherwise alter such information with malicious intent.
- Engage in any illegal activity, unacceptable behaviour or activities which may bring discredit to UBC.
- Downloading video and music files where work benefits do not accrue.
- Engage in any personal, for profit activity including but not limited to offering services or merchandise for sale.
- Represent themselves anonymously or as someone else, whether real or fictional, when sending mail or posting information to an internet repository.
- Make illegal copies of protected material.
- Disrespect the privacy of other internet users or engage in any activity that affects their right to confidentiality.
- Harm or attempt to harm data or system files being used by or owned by any other internet user.
- Post any defamatory comment.
- Circumvent copyright provisions.
- Maintain or support a personal private business.
- Perform unsolicited mass marketing on the internet (spamming).

Inappropriate use of the internet can lead to disciplinary action and/or the revocation or suspension of internet access. Any staff found to have used UBC's owned communication or information device to download, store or distribute pornography will be dismissed.

Personal use of the internet

Limited personal use of the internet is permitted where it:

- Generally takes place during the employee's non-work time
- Incurs minimal additional expense to the company
- Is infrequent and brief
- Is not used to support a personal or private business
- Does not interfere with the operation of the company
- Does not compromise the security of the company systems
- Does not violate State/Federal legislation and regulation

Examples of limited personal use include:

- Accessing non-work related sites during a lunch break
- Briefly accessing a non-work related site during office hours, similar to making a brief personal phone call

Monitoring Internet Usage

All use of the internet will be monitored from time to time. A log of internet access is recorded and archived regularly. Access to the log will be strictly controlled and used for monitoring internet usage.

EMAIL USAGE

Ownership

UBC owns all corporate electronic mail systems, including the information being sent through them. The e-mail services have been provided for business purposes and messages should be confined to business matters only.

Rights and responsibilities

All staff are responsible for their use of email and will be held accountable for all messages issued in their name.

Usage Guidelines

- Mail should be checked regularly. Ignoring messages or deleting messages without reply can be discourteous and confusing to the sender.
- If you are out of the office and will not be reading your mail regularly, ensure that an "out of office" message is organised in your Outlook. The message should provide alternative contact details so that queries can be forwarded to someone within the office.
- You should manage and clean your mailbox regularly.
- You should endeavour to achieve a professional style in your email. The use of colour rich message templates and signatures adorned with graphics or clipart must not be used. Email signatures are managed by State Committee and all follow a branding style which must be kept to.
- All documents emailed externally must be sent as a PDF format.

- Sensitive information can be easily disclosed via email. Never send or keep email that you would be worried about being quoted, printed or forwarded onto others.
- Staff do not have a personal privacy right in any matter created on, received through or sent from the company email system. Employees and Directors should not enter personal matters into the email system.
- Treat email as a permanent, official record. What you write can be used in evidence for or against you. Keep this in mind before you click the send button. Even if you don't think the matter is important enough to keep a copy, your recipient may. Assume that any message you send is permanent and could be modified and or forwarded throughout the world without your knowledge or consent

Email Etiquette

A misinterpreted email can lead to strained relationships with colleagues, wasted time and unnecessary delays. Without face to face communications, comments in email may be viewed as criticism. Be polite, professional and careful about what is said in an email; especially about others (the informality of email can trick the unwary).

Principles to consider when using email:

- Your emails may not be read in the way you intended. Writing in capitals and using exclamation marks looks like you are shouting, being aggressive in nature, making fun of the recipient or not taking them seriously.
- Even if an email was not intended to be offensive, the recipient may deem it as inappropriate. If in doubt, it is best to leave it out.
- Although an issue at hand may be important to the sender, it can be seen as unnecessary to send it to all within the organisation or multiple colleagues. It is best to send an email to those directly involved in the matter.
- Although a task may be deemed to be urgent to the sender, using capitals and red letters does not mean that the recipient will view it as the same. Use a subject line that reflects the task factually and ask politely in the email when the task can be scheduled in.
- Inappropriate use of Email
- Do not send messages or components which are libellous, defamatory, abusive, discriminative, obscene or in bad taste. No e-mail message should be created or sent that may constitute intimidating, hostile, or offensive material on the basis of sex, race, colour, religion, national origin, sexual orientation or disability. UBC policy against sexual or other harassment applies fully to the email system, and any violation of that policy is grounds for discipline up to and including discharge.
- Do not send large file attachments. This can lead to server and network congestion and degraded performance. The limit for attachments is 5MB when sending to internal staff. No mail greater than 2MB should be sent to external recipients.
- Obey copyright laws. Do not distribute software, games, or other material that may infringe copyright laws. UBC has a legal responsibility to enforce copyright law and offenders will be prosecuted.

EXTERNAL SOCIAL MEDIA

Standards in relation to Blogs and Sites not operated by UBC

UBC acknowledges that users have the right to contribute content to public communications on websites not operated by UBC, such as social networking sites like Instagram, Snapchat, LinkedIn, Facebook or YouTube. However, inappropriate use of such communications has the potential to cause damage to UBC, staff, members, volunteers, partners and suppliers. For that reason, the following provisions apply to all users.

As it may not be possible for any user of an external site to conduct a search that will identify any blogged comments about UBC, users must not publish any material which identifies themselves as being associated with UBC.

Users must not publish any material that may expose UBC to any possible legal liability. Examples include, but are not limited to, defamation or discrimination proceedings.

Blogging Facility

UBC website includes a blogging facility that only authorised users may use.

Authorised users are only permitted to contribute to blogs on UBC's website in order to share information and knowledge, obtain constructive feedback, interact directly with members, volunteers and partners, collaborate over projects and solve problems, promote our organisation, and raise UBC's profile.

Standards in relation to Blogs and Sites operated by UBC

Users must not engage in prohibited conduct. Further:

- Only users who are authorised by State Committee are permitted to publish a blog on any sites operated by UBC and the content of any such blog must first be approved by UBC before publishing.
- Public communications concerning UBC must not violate any provisions of any applicable policy, procedure or contract.
- A user may participate in related public communications during normal work time. However, if doing so interferes with any of the user's normal work responsibilities, UBC reserves the right to withdraw the user's access to the communication facilities.
- A user must not communicate any material that violates the privacy or publicity rights of another party.
- A user must not cite or refer to committee members, business partners, suppliers, other users etc without their prior approval.
- A user may respectfully disagree with a Person's actions, policies, or management, but must not make personal attacks on any Person
- Users will be personally legally responsible for any content they publish and need to be aware of applicable laws.
- If the user subsequently discovers a mistake in their blog, they are required to immediately inform and then take steps authorised by UBC to correct the mistake. All alterations should indicate the date on which the alternation was made.

Apart from the potentially damaging effects a blog may have on UBC, inappropriate blogs on internal or external sites can also have adverse consequences for a user in terms of future career prospects, as the material remains widely and permanently accessible to other site users.

Monitoring and Management

- State Committee will ensure that all staff are aware of their rights and obligations under this policy.
- All persons intending to use the UBC's internet, email and computer facilities will be required to read and sign this an acknowledgement of their understanding and adherence to the internal systems and that gateways will be monitored, and activities will be logged.
- Messages and systems can and will be audited from time to time.

Breach of Policy

Breaches of this policy are not acceptable by any employee and will be responded to promptly. Serious breaches of this policy may result in disciplinary action, including up to dismissal.

Review

This policy and related procedures will be reviewed every three years, unless changed circumstances require earlier review.

Associated Policies, Procedures and Other Documents

- Privacy Policy
- Retention and Storage, Record Keeping policy

References

- N/A

Policy Name: Information Technology Policy

Responsible Director: State Committee

Functional Area: Organisational

Date adopted: 26th April 2020

Review Date: 26th April 2023

Review History

Date	Review Details	Action
06/04/2020	Major update of policy to incorporate updated technology and incorporated social media use	Updated, reviewed and ratified

INFORMATION TECHNOLOGY POLICY

I confirm I have read and understood the Information Technology Policy

Staff Signature …….. Date ……

Print Name …….