INFORMATION TECHNOLOGY (IT) POLICY

Change begins with Education

Table of Contents

IT POLICY

1. PURPOSE

This policy prescribes the standards to be applied by stakeholders when using IT equipment, data storage, or digital communications mediums as used by or made available to staff for the purpose of carrying on their roles and responsibilities. In many cases, but not all, SeeBeyondBorders has provided a computer (or laptop) and associated hardware to staff to use for work purposes. The purpose of this policy is to:

- Ensure that IT equipment is always in good condition and work related documents are stored securely.
- Ensure that SeeBeyondBorders staff are accountable for the use of computers and work related documents.
- Ensure that SeeBeyondBorders adheres to essential regulatory requirements, and basic industry standards.
- Ensure SeeBeyondBorders and its staff comply with the state and federal laws of the jurisdictions where we work.
- Ensure SeeBeyondBorders staff use ONLY the software we provide for their work.
- Ensure SeeBeyondBorders staff store documents securely in the cloud.
- Ensure no internal document is copied outside the organization.
- Ensure that our software and/or licenses are safe from hacking or stealing.

2. DEFINITIONS

Information Technology (IT) Equipment: This refers to hardware that is purchased by SBB for the use of staff members that assembles, stores, correlates, or otherwise processes information to be captured, stored and/or distributed electronically. This includes, but is not limited to:

- Computers – Desktop PC, Laptop or Mac
- Computer accessories – power cable, mouse, keyboard, speakers, etc
- USB Internet Modem (Dongle)
- External USB Hard drive
- Printers, scanners
- Projector

Software: Refers to the apps installation or a web application on computers or mobile devices, such as Microsoft windows, MacOS, Microsoft office.

G-Suite account: Refers to the account created on G-suite to use google service, such as email, calendar.

Third party software: Refers to other applications or web applications installed or used in computer or sign in to web browsers, such as Google Chrome, Xero , Harvest.

Anti-virus: Software developed to detect and remove computer viruses, such as McAfee, Avast, ESET.

Google Drive (or partition G): SeeBeyondBorders store most of their files on the cloud storage which belongs to Google. Google Drive file stream is installed on all computers to ensure easy access to files on the cloud. Users can also access the drive through drive.google.com on the web browser.

Drive D (or partition D): Drive D is not actually another hard drive, nor is it the letter or name as assigned to a memory-card slot. It is a partition of your primary hard drive, a separate area created especially to hold certain files or data for use as a backup in case of corruption or problems with the primary C Drive. In some SBB computers there is no Drive D partition.

3. POLICY

This Policy should be read in conjunction with the Privacy Policy which sets out SeeBeyondBorders approach to the use and retention of private and personal information and the use of Coolies and provides reference to the relevant legislation. Policies in this document are as follows:

3.1. Staff who have been allocated SBB IT equipment are responsible for ensuring the ongoing care and maintenance of these items. It is a requirement to ensure these items are safely stored away from potential damage or theft. For example, storage away from windows, not leaving it in an area that can be exposed to water, overheating, etc. Equipment should be stored safely at the end of each day.

3.2. SeeBeyondBorders equipment is set up with an anti-virus program. This software must be set up to automatically update on a weekly basis and conduct virus scans daily/weekly. It is strongly recommended that a Full Scan setting is used every time.

3.3. If any IT equipment is broken and needing repairs, the responsible staff member must inform the Administrative Officer or I.T Manager in advance of seeking repairs. The cost of repairs will be reimbursed to the staff member on production of a detailed receipt.

3.4. All staff should save work-related documents into Drive G (Personal Work Drive) or related work documents in specific departments such as: Administration, Finance…. in SBB New Drive, not to Drive C or Desktop. This method of saving the data will prevent files being lost from the local hard drive or if any incident happens to the computer.

3.5. Staff should save work–related documents in Google Drive and should not store personal documents in SeeBeyondBorders' I.T Equipment.

3.6. Staff are permitted to take computers and accessories home outside of work hours, however they will be responsible for any loss or damage incurred outside of work activities.

3.6.1. Staff are responsible for ensuring the safety and security of SBB IT Equipment at ALL times, both during and after work. If SBB IT Equipment is subject to theft or unforeseen criminal acts at any time (i.e. stolen from outside a school, or someone breaks into house at night, or your house and possessions are damaged in a fire), the responsible staff member must obtain a police report stating that the incident occurred despite all reasonable care being taken. The cost of replacement will be equally shared between the responsible staff member and SBB (50% of replacement value each) subject to the discretion of the CEO or his delegate.

3.6.2. If a computer or IT equipment is damaged or lost during a natural disaster, i.e. storm, war, flooding, etc., the staff member who had care of the equipment shall not take responsibilities for such damage and loss. This is considered to be beyond any reasonable control of either the responsible staff member or SBB.

3.7. Staff shall not lend SBB IT equipment to their friends or relatives to use without permission from CEO or Country Manager. If staff have been permitted to lend SBB's computer to friends or relatives, staff must ensure that confidential work-related documents of SBB are protected/or locked in the safe folders which cannot be accessed by non-staff members.

3.8. Staff may only use their SBB-issued IT Equipment for **limited** personal use, where it is infrequent and brief and does not:

3.8.1. Interfere with their duties or that of their colleagues.
3.8.2. Interfere with the operation of or compromise the security of SeeBeyondBorders.
3.8.3. Impact on SeeBeyondBorders' electronic storage capacity or decrease network performance.
3.8.4. Incur any additional expense for SeeBeyondBorders.
3.8.5. Violate any laws or compromise any confidentiality requirements of SBB.
3.8.6. Require installation of unsecured or untrusted software applications

3.9. Staff may not use email or access the internet on IT Equipment provided by SBB to:

3.9.1. Create or exchange messages that are offensive, harassing, obscene or threatening.
3.9.2. Access, view or store objectionable (including pornographic) or criminal material.
3.9.3. Create, store or exchange information in violation of copyright laws (including the uploading or downloading of commercial software, games, music or movies).
3.9.4. Use internet-enabled activities such as gambling, gaming, conducting a business or conducting illegal activities.
3.9.5. Create or exchange advertisements, solicitations, chain letters and other unsolicited or bulk email.
3.9.6. Or any action which may breach the SBB Marketing & Communications policies

3.10. At no time are staff permitted to share, either electronically or hard copy, any work-related documents of SeeBeyondBorders to any person external to the organization without express written permission from SeeBeyondBorders senior management, in advance. If a third party requests any documents from SeeBeyondBorders, staff are required to refer such requests to the CEO and Country Manager.

3.11. If the equipment has software issues or hardware issues staff should contact the I.T Manager on helpdesk@seebeyondborders.org to get help and advice.

3.12. IT equipment used by staff, volunteers and stakeholders must use a complex user password login to ensure it is safe from other people. It is recommended that passwords are at least 8 characters long and contain at least one of each: upper case letters, lower case letters, and a number and a symbol. For example: Camb0dia!

3.13. Staff and volunteers should not share passwords or login details of software that SeeBeyondBorders provides to each other or to anyone outside the organisation. When emails are accessed on mobile devices, staff must set the login passcode/password on those devices to be secure. It is also recommended that staff install anti-virus software on any mobile phones used to access SBB documents and communications.

3.14. Staff who have Administrator rights of SeeBeyondBorders software such as Xero, Harvest, Flickr should change the password regularly and password must be complex in order to make sure no one outside SeeBeyondBorders is able to access the content.

3.15. I.T Equipment used by staff or volunteers in SeeBeyondBorders will be tested and serviced at least once every year. It is the responsibility of each staff member to arrange for servicing annually. This will be tracked by the IT manager for audit purposes.

3.16. New staff or volunteers who start with SeeBeyondBorders will receive an IT induction session. Also when staff leave, there will be an IT exit interview session. The I.T manager will document in Information Technology Systems_ITS in SBB NEW Drive.

3.17. Software or licences used in SeeBeyondBorders needs approval from Finance on recommendation from the relevant manager and in accordance with the purchasing Policy and Budget Management authorities as held at different levels by the Leadership Team.

3.18. SeeBeyondBorders' Educational Technology program works with stakeholders such as teachers and school principals, and SBB delivers IT Equipment such as tablets, Projectors, and Internet modems to implement the program. IT Usage agreements must be drawn up and adhered to with those stakeholders to whom equipment is provided identifying that it is only for use under the prescribed conditions. Should the user withdraw from any SeeBeyondBorders program to which the equipment is attached, the equipment must be returned.

3.19. IT Equipment and Software are designed to perform a regular software update. If the software prompts the user that it needs an update, staff are required to regularly update those software changes to enhance security on the devices.

4. BREACH OF POLICY

A breach of the IT Policy by SBB staff will result in disciplinary action ranging from verbal and written warnings to termination and possible referral to local authorities. The decision on appropriate disciplinary action will be made by the Line Manager in co-ordination with senior SBB Management and in line with the SBB HR Manual. The discussion on the termination of the employment will be conducted as per the terms set out in the employment contract.

5. POLICY MANAGEMENT

This Policy has been approved by the Australian Board and the Trustees of SeeBeyondBorders' other entities as noted below.

Amendments and or developments will be recommended to the Board from time to time as deemed appropriate by senior management. Formal reviews will take place before the expiry of three years from the anniversary date of approval by the Board. Recommendations for minor changes can be approved by the CEO before the expiry of three years, and recommendations for changes to the background or policy in practice can be approved by the relevant Sub-Committee.

Doc ref	Doc type	Approved by Australian Board Date	Minute ref.	Approved by UK Trustees Date	Minute ref	Approved by Irish Board Date	Minute ref
	Policy Original	2015		N/A	N/A	N/A	N/A
ITP/06/2020/1.0	Policy Review	29 June 2020	Item 8	22 July 2020	Item 5		