ICT Acceptable Use Policy

Date: December 2019

Level 9, 117 Clarence Street
GPO Box 10500
Sydney NSW 2001

Telephone 02 9085 7222
Facsimile 02 9085 7299
thesmithfamily.com.au

Contents

1 Introduction

There are legal, financial and reputational risks to The Smith Family (**TSF**) if persons associated with the organisation use Information and Communication Technology (**ICT**) in an inappropriate manner. This ICT Acceptable Use Policy outlines the acceptable use of TSF's ICT so as to mitigate those risks.

2 Purpose

The purpose of this ICT Acceptable Use Policy is to provide a clear and concise statement to all persons associated with TSF (see Scope) on the acceptable and unacceptable use of ICT equipment and facilities at TSF.

3 Scope

This Policy applies to all personnel who have access to The Smith Family ICT systems (Personnel). This includes all employees, contractors and volunteers, regardless of position, level of seniority or location within the business. Furthermore, this includes third parties, including corporations or individuals, sub-contractors or parties engaged by any external service provider with whom The Smith Family has a commercial relationship, and who require access to The Smith Family systems or data for the completion of their role.

4 Key Principles

The following provide the overarching principles to be followed by all Personnel with access to TSF's ICT systems or data. Specific guidance and examples then follow.

Principle	Description
Business first	ICT assets and services are made available to Personnel to perform their duties for TSF. Limited personal use is permitted provided it does not interfere with the performance of those duties.
Protect our interests	ICT resources should not be used in a way that could cause TSF damage, embarrassment or loss, or to promote interests other than those of TSF.
Approved components	Only authorised equipment, software, and services can be introduced and used in the TSF environment.
Lawful use	The Smith Family ICT assets and resources can only be used for lawful activities, and cannot be used for any activities which would contravene any laws or regulations such as rules and obligations about: • Privacy; • Discrimination; • Child protection • Confidentiality. • Defamation; • Copyright; • Harassment, intimidation or bullying; and
Report issues	If you see something that doesn't appear right, let the BIS team know. Security is everyone's responsibility. Contact your manager and the BIS Support Desk
If in doubt, ask	If you are not sure about specific access or use of ICT assets, services and information, or whether you're doing the right thing, get in touch with the BIS Support Desk. We're happy to clarify.

5 General Responsibilities and Applicability

The following sets out TSF's general expectations around ICT Acceptable Use along with key rights and obligations:

- The Smith Family embraces and relies on the use of technology, the Internet and digital media in the conduct of its business.

- The Smith Family expects the Personnel who have access to its ICT facilities and services to use them in a professional manner whilst adhering to the organisation's policies and procedures, including this Policy.
- The Smith Family expects its Personnel to use ICT for purposes consistent with their duties and to follow any reasonable directions that are issued from time to time by BIS team including in relation to passwords, protection against cyber threats.
- The Smith Family reserves the right to access any email sent on or through its networks.
- The Smith Family reserves the right to monitor Internet activity (including email, web browsing and applications) on a per user basis.
- Any Personnel who are found to have contravened any part of this Policy, may be subject to disciplinary action that may include termination of employment, termination of contract, and/or legal action.
- All individuals requiring access to ICT services provided by The Smith Family must confirm their acceptance of this Policy before using these services.
- The Smith Family takes no responsibility for digital content that Personnel download, store or use on their The Smith Family devices. As required, The Smith Family will assist any State and Commonwealth Law enforcement authority in their investigations involving Personnel suspected of unacceptable use which potentially involves a breach of laws or regulations.

6 Specific Guidance

Social Media

- The following outlines the acceptable use around social media at The Smith Family: Social media including Facebook, Twitter, wikis, blogs, YouTube and LinkedIn can be useful workplace resources. All Personnel are expected to act responsibly when using these sites and comply with this Acceptable Use Policy.
- When accessing and contributing on social media:

What to Do	What Not to Do
Be cautious of the integrity and accuracy of information accessed via social media – confirm authenticity before relying on it.	Represent or give the impression of representing The Smith Family when you're not authorised to do so.
Protect The Smith Family data at all times, in accordance with the TSF Information Asset Classification and Handling Policy	Access or distribute content that isn't fit for a working environment - pornography, gambling, discriminatory or other content which may be considered offensive.
Be mindful of TSF's status as a registered charity that is independent, non-religious and non-political	Post a comment which implies that The Smith Family is affiliated with any political party or candidate, or which espouses or directly associates TSF with the views of a religious organisation.

Email & Internet Security

The following outlines the acceptable use around Email and Internet Security at The Smith Family:

- Email and Internet facilities provided by TSF are intended for official use as required by the recipient's job description and responsibilities. Limited personal use of Internet and email is permitted provided it does not interfere with the discharge of your role.
- Each person is responsible for any digital content that they store on their The Smith Family devices or send over The Smith Family email system or network.
- When using The Smith Family's email and Internet access:

What to Do	What Not to Do
Be cautious of email asking you to open files, click links, or release information. If in doubt about the integrity of a message, attempt to contact the sender by phone or get in touch with the BIS Support Desk for advice.	Attempt to change or circumvent any security controls on an IT system without proper authorisation from the IT team.

Use The Smith Family email account for all official TSF business only.	Use your TSF email for any business activities other than related to The Smith Family, or for any political or religious activities.
Regularly clear your Inbox of any personal messages.	Include a work-related sign-off or signature on a personal email.
Immediately report to the BIS Support Desk if you receive digital information you are not authorised to receive or the information appears illegal or otherwise inappropriate.	Download any obscene digital material or pornography
Always access The Smith Family sites requiring authentication (i.e. User ID & Password) by entering the URL into the browser bar or using your browser's bookmarks.	Hide your identity, or claim to be someone else, or claim to represent someone else, unless explicitly authorised to do so.
Get authorisation from the BIS Support Desk prior to installing any software on a device issued to you by The Smith Family.	Send messages that are hateful, harassing, or threatening or that support illegal or unethical activities.
Notify the BIS Support Desk if you receive a suspicious email message.	Put any TSF Password at risk by sending it in clear text by email, or by re-using it for any system outside of The Smith Family.
	Transmit unsolicited mass email (spam).

Data Storage and Management

- Ensuring that information and data is securely stored and managed is critical to our reputation and ongoing success. At the same time, we must also respect the data and intellectual property of third parties in our day to day operations.
- All Personnel who obtain access to other companies' or individuals' information, materials or other data must ensure that copyright is observed and may not copy, retrieve, modify or forward copyrighted materials, except in a manner consistent with relevant licence terms or with permission of the copyright owner, or as may be otherwise permitted by law.
- TSF's information management systems are costly to maintain. Before downloading or storing material on TSF ICT equipment or devices please consider whether you are doing so for legitimate TSF purposes and whether it is necessary for the discharge of your role.
- When storing or transferring data:

What to Do	What Not to Do
Ensure that you have a legitimate license for any software or digital content subject to copyright stored on your personal C: drives.	Store prohibited or inappropriate material, or so much personal material as to interfere with business use, on their personal C: drives.
Ensure that any data not explicitly defined as 'Public' is subject to suitable controls (as defined by the classification of the data) prior to being taken outside The Smith Family's physical and logical boundaries.	Store, transmit or otherwise take any data not explicitly defined as 'Public' outside The Smith Family's physical and logical boundaries without approval from the IT team.
Ensure any USB drives or other external storage media connected to an The Smith Family system, is subject to a malware scan on connection and prior to use.	Supply any non-Public data to third parties without suitable legal and technical controls in place, to protect the interests of TSF its staff, customers and partners.
Only use licensed software officially installed/registered as owned by The Smith Family.	Store large personal files such as graphics, music or video files on any network drive.
Only use the applications to which you have authorised access.	Store, transmit or make available unauthorised copies of copyrighted material using any The Smith Family computers, networks or storage media.

Manage your personal information security 'hygiene' (e.g. lock your screen when away from your PC and choose strong passwords).	Make illegal copies of copyright material, specifically including – but not limited to – software programs, music files or video files.
Ensure all Personnel who have access to the personal and sensitive information of children have the required training and clearance including a satisfactory Working With Children Check within their jurisdiction.	Install or use any unauthorised software or software that you suspect to be unlicensed.
	Connect any personal IT device to The Smith Family network environment without authorisation.

Monitoring and Logging

- The Smith Family is subject to various laws and regulations, as well as being a significant target for cyber criminals. It is imperative that we maintain a close watch on our systems, networks and data, and we do this through both technical and procedural controls.
- The Smith Family conducts active and ongoing monitoring and logging of the use of The Smith Family ICT devices, networking equipment, and other ICT services for the purposes of ensuring compliance with The Smith Family policies, local and international laws, regulations and other obligations.
- The Smith Family's monitoring may include, but is not limited to:
    - Maintaining logs, backups and archives of computing activities including workstations, laptop computers, servers, printers, and network connected devices, including TSF issued smart phones.
    - Monitoring and retaining emails and attachments sent and received through TSF servers including where these have been deleted by Personnel.
    - Monitoring all Internet access and network usage and retaining logs, backups and archives of the same including URLs or website addresses of sites visited, the date and time they were visited and the duration of site visits and logs.
    - Reviewing installed software, files and metadata on any and all TSF supplied or sourced ICT assets.
    - The BIS team will periodically audit systems to ensure compliance with this Policy, our other IT Security Policies and other TSF Policies. You must respond to any requests by the IT team to provide evidence of your compliance including software licences for any non-standard software loaded on your PC or laptop.
    - Unauthorised digital content may be subject to quarantine or immediate removal by the IT team.

7 Related Documents:

Other TSF Policies may be relevant to your use of ICT. Please refer also to:

- TSF Information Security Policy
- TSF Information Asset Classification and Handling Policy
- Code of Conduct
- Social Media Policy
- Child Protection Framework

8 Security Incidents

- Security Incidents are adverse events that pose a threat to The Smith Family information systems and services. Such incidents can originate from intentional or unintentional actions (human errors).
- The Smith Family has established an Incident Management Standard for the timely and effective handling of information security incidents. Examples of potential security incidents include:
    - Abnormal computer behaviour which might be caused by malware.
    - A non-escorted guest at TSF premises.
    - Disclosure of information to unauthorised persons.
    - Loss of devices, removable media, passwords or data.
    - Unauthorised access to an information system or physical premise.

What to Do	What Not to Do
Report a suspected security incident immediately to BIS Support Desk on +61 02 9085 7111. Complete a Child Safety Alert where you suspect the personal and sensitive information of children or young people has been accessed in a manner that could lead to abuse or otherwise accessed for improper purposes.	Perform any action (e.g., delete system files) to eradicate or contain a suspected security incident unless explicitly instructed by the IT Team.
In the event of a physical security incident, follow all established action and escalation procedures as soon as reasonably practicable.	Disclose information relevant to security incidents to unauthorised persons.

9 Definitions and Document information

Term	Definition
ICT Equipment	All equipment which has an IT based function associated to it in the organisation.
BIS	Business Information Services. The IT team of The Smith Family. Phone: 02 9085 7111.
Licenced Software	Software that has been purchased for use with a legitimate licence for operation in the business.
Digital Content	Any content that is electronic and is processed and stored with ICT systems within the organisation.
Social Media	Tools and applications that enable users and business to create and share content to the outside world.
Public	Information that can be freely used, reused and redistributed by anyone with no existing local, national or international legal restrictions on access or usage

Document Details				
Document Name	ICT Acceptable Use Policy			
Document Author	CISO – Andrew Wan			
Document Reviewer	CIO – Mathews George			
Document Approver	Data & Technology Governance Group (DTGG)			
Date of Approval	23/01/2020			
Review Frequency	Annually			
Version No.	**Version Date**	**Details**	**Amended By**	**Approved By**
1.0	09/01/2020	Updated ICT Acceptable Use Policy (Draft)	Andrew Wan	DTGG