GWF / George Weston Foods Limited

Information Systems Use Guideline

Effective date	20th December 2017
Policy owner	Group Finance
Applies to	All GWF employees, contractors, customers, visitors and related entities of GWF supported by IS.
Contact Officer	GWF IS Director

This Guideline confirms our commitment to making GWF workplaces professional for ALL.

Purpose and aims

George Weston Foods Limited, George Weston Foods (NZ) Limited and their related companies (**GWF, we, us, our**) understand that the increased use of information systems and the internet in the workplace has given rise to a range of issues, including the risk of access to inappropriate material and difficulties protecting confidential information, which we need to properly address.

This Information Systems Use Guideline (**Guideline**) addresses these issues in our workplace by providing guidance as to what is and is not an acceptable use of information systems at GWF. This Guideline supports and should be read in conjunction with the **Information Systems Use Policy**, **The Red Book** and the **ABF IS Security Policies**. If you are an employee, contractor or third party who makes use of IS provided by GWF (user, you, your), this Guideline applies to you and you must familiarise yourself with, and comply with, this Guideline and any variations to this Guideline.

This Guideline may be reviewed, varied, added to or withdrawn by GWF at any time, at our absolute discretion. This Guideline, and any amendments to it, does not form part of your employment contract or independent contractor agreement (as the case may be).

Information systems

Information systems (**IS**) at GWF include:

- all our assets (tangible and intangible) including data, computers, telephone and electronic equipment and devices, personal digital assistants and other electronic communication technologies including wired and wireless networks, personal mobile devices including smart phones and slates/tablets, supporting servers and all associated software and hardware (**Assets**); and
- all operating systems or other systems supplied by us or are accessed using Assets, including our networks, remote access networks, internet, e-mail, mail storage or any form of communication systems and IS facilitated processes such as financial, backup and recovery, availability, project design, business continuity and disaster recovery, governance, procurement, auditing, and licensing (**Systems**)

Users are defined as any person that uses any GWF Assets or Systems, and can include GWF's employees, contractors and third parties.
GWF Policies means any policy of GWF as updated or introduced from time to time. These policies can be found on the GWF Intranet (The Zone).

Introduction

GWF Information Systems play a major part to support and protect GWF and its clients to ensure the ongoing success of the company. It is essential for us to ensure that the integrity, confidentiality and availability of our Information Systems are in line with the requirements of our business, accepted standards of best practice and current legislation.

The aim of this Guideline is to ensure that all Users understand their responsibilities in relation to the ownership, use and security of that information.

Specifically, the Guideline requires that all Users be fully aware of their own responsibilities and the potential consequences of:

- Committing breaches of confidentiality in relation to GWF information
- Loading or using unauthorised software on GWF owned computers or systems
- Making unauthorised access to, or misusing of the Internet

It is intended that this Guideline will ensure that the GWF approach to protecting our Information Systems is proactive and in line with ABF Policy. This guideline aims to focus on the following areas:

- Scope
- Legal Responsibility
- Rules governing the use of GWF computer systems
- Logging and resolution of Security Incidents

We all have an interest in ensuring that GWF Systems and Assets are not abused or misused. Your co-operation in the implementation and adherence to this guideline will help to achieve this. If you have any questions or require clarification of these guidelines, please ask your line manager or the GWFIS Service Desk.

Legal Responsibility

GWF has legal obligations under Australian law which relate to the use of information systems including the *Criminal Code Act 1995* (Cth), the *Cybercrime Act 2001* (Cth), the *Telecommunications Act 1997* (Cth), the *Privacy Act 1988* (Cth), the *Spam Act 2003* (Cth), *the Copyright Act 1968* (Cth) and the *Patents Act 1990* (Cth). GWF endeavour to implement procedures and practices in line with the laws and, where a breach has taken place, take appropriate action wherever possible.

Care of Assets and Systems

All Users must follow all instructions about how to use and care for GWF Assets and Systems. Systems and Assets are business tools and are provided for GWF business purposes and must only be used:

- for GWF business purposes, except as otherwise set out in this guideline or the GWF IS Use Policy
- and in a professional, appropriate and lawful manner

GWF may, as a matter of discretion, allow the use of Systems or Assets for other purposes, if the use does not adversely impact work performance and does not breach any GWF Policies. GWF may also cease or restrict access of specific people or to specific Assets and Systems at any time.

Accountability

All Users are issued with a unique username and password which the individual must treat as strictly confidential. Everyone is solely accountable and responsible for all actions performed under the username and password. GWF may hold you responsible for any:

- damage to or unlawful or illegal use of Assets or Systems;
- costs incurred by your access to internet sites or any other system;
- and/or any legal obligation to any person created by your use of the Assets or Systems;
- any other breaches of GWF Policies

When using Assets and Systems, All Users must:

- always identify yourself clearly and honestly;
- not tell anyone your password;
- and never access another person's email, social media or internet account without that person's permission

Network passwords are subject to a regular replacement period and should be reset when requested. This ensures secure passwords are in place to protect against unauthorised access.

System Owner / User Responsibility

Users must ensure that when a computer is unattended all available steps are taken to prevent unauthorised access, damage or theft. GWF data must be stored only on authorised GWF mobile devices under Mobile Device Management.

When travelling, laptop computers are particularly vulnerable to theft. They should, therefore, always be carried as hand luggage and must not be left unattended in public places. Laptops must NEVER be left in an unattended car when parked or overnight.

To prevent unauthorised access, damage or theft, Assets must be secured by all reasonable means. It is a GWF requirement that any loss or theft must be reported to the police and a reference number obtained. Users must also immediately notify the GWFIS Service Desk and their line manager of any loss, damage or theft to ensure that all Assets are secured as soon as practicable.

Prohibited uses

Whilst the IS Use guideline should generally be applied, Systems and Assets must not knowingly be used to or attempt to be used to (without limitation):

- store, copy or otherwise share digital information or media that is subject to copyright where it cannot be proven that:
    - the copyright to the material is owned by either the individual or corporate entity; or
    - explicit permission has been granted by the copyright owner to use, copy, store or share the material;
- participate in file sharing technologies for the practice of distributing or providing access to copyrighted material. File-sharing technologies are defined as any storage, transmission, distribution model and automated sharing such as peer to peer networking technologies, non GWF shared document technologies such as web-based forums or web-based document sharing, blogs, wiki's and manual sharing using removable media, centralised computer file server installations (within a computer network);
- engage in illegal or fraudulent acts, or be part of an unlawful activity; make or infer slanderous, libellous, and/or defamatory statements; act in ways that are offensive, obscene, pornographic, or in bad taste; be abusive and/or threatening of violence; incite any person to break the law;
- engage in harassment, bullying or unlawful discrimination; disable or delete virus protection software;
- sending, receiving, displaying or accessing material that is, or may be construed to be, obscene, derogatory, defamatory, harassing, threatening, vilifying, racist, sexist, sexually explicit, pornographic, or otherwise offensive or excessively personal;
- send unsolicited email, including selling or chain emails (defined as email that the recipient has not granted permission for the message to be sent); promote personal views, interests and beliefs that are unrelated to your GWF role; injure the reputation of or cause embarrassment to GWF or its brands; send or receive material relating to the manufacture, use, sale or purchase of illegal drugs or dangerous materials or to any other illegal activity;
- send or receive, print or otherwise disseminate confidential information, without prior authorisation and appropriate security measures in place (e.g. data encryption techniques); infringe the intellectual property rights of another person; distribute unauthorised software; give

passwords to others, except as indicated elsewhere, operate on another User's password or falsify an identity to others while using the Systems;

- supervise, manage or operate for commercial purposes other than GWF business; gain access to another's (employees/company's) resources, programs, or data without requisite authority;
- vandalize, including any attempt to harm or destroy data of another User on the Internet, and includes but not limited to the uploading, modification, downloading or creation of data which includes computer viruses; game, wager or bet; engage in political lobbying; contribute to electronic bulletin boards or internet chat rooms; perform any activity using an anonymous or misleading identity; intentionally evade GWF monitoring; or do anything that violates any other GWF guideline or policy.

Software downloads and management

Software (licensed, shareware, freeware, evaluation or otherwise) including system, application or data files may only be downloaded using procedures approved by GWFIS. Under no circumstances may software be installed to Systems or Assets if it has not been approved by the IS Team. All software used on GWF Information Systems must be appropriately licensed. Only approved GWF business software is to be installed and operated on GWF owned computer hardware.

No games or any private software are to be loaded to any GWF computer other than those embedded within standard operating systems, nor should they be loaded onto any other the Assets or Systems.

Only approved persons within GWF are permitted to download, load or install third party software or data for evaluation, testing, virus checking and installation.

Viruses

Mail virus checking is done automatically through the software installed on the mail server. All Users that are concerned about an email attachment, or believe that it has not been automatically scanned for viruses, you should contact the IS Service Desk.

All GWF owned computer systems will have automatic virus scanning routines. These routines must not be cancelled or altered in anyway. Disabling local security and malicious software protection will be considered a disciplinary offence.

Any failures of such virus protection methods must be reported to the GWFIS Service Desk immediately.

Any computer system not running automatic virus protection updated to the latest patch or definition level is prohibited from connecting to the GWF Corporate network. All users are advised to contact the IS Service Desk if you are uncertain.

Intellectual Property

When using Assets, or distributing information over the Systems to third parties outside GWF, All Users must ensure that GWF and the individual have the right to do so and that you are not violating the intellectual property rights of GWF or any third party.

This applies when copying information or downloading software. Copyright law may apply to the information you intend to distribute or copy, and must always be observed. The copyright material of third parties (for example, software, database files, documentation, cartoons, articles, graphic files and downloaded information) must not be distributed through email without specific authorisation to do so, or under very limited conditions. If you are unsure whether you are permitted to distribute or copy specific information, you should contact the GWF Legal team.

Social Media

Social media should not be used to discuss or store any confidential or sensitive company information (such as financial information, future business performance, business plans, innovation plans and people movements). GWF recognises both the importance of social media as a tool for engaging with our customers and our people and the need to "empower and trust" our people to use these tools responsibly. However, communication on social media that could be deemed to represent the opinion or view of GWF must be authorised.

If you are authorised by GWF to create, monitor or post on a social media page for the business, then you must follow any directions about content provided by your manager as well as the guidelines set out in this document. You must keep any passwords used to access business related accounts secure, but always ensure that your manager has access to such logins and passwords. You should never use business accounts for personal purposes or outside of your role or after termination of your employment.

For this guideline, web-based tools include but are not limited to:

- social networking sites e.g. Facebook
- video and photo sharing websites e.g. YouTube, Tumblr, Instagram
- micro-blogging sites e.g. Twitter
- weblogs, including corporate blogs, personal blogs or blogs hosted by traditional media publications
- forums and discussion boards such as Whirlpool or Google Groups
- online encyclopaedias such as Wikipedia any other web sites that allow individual users or companies to use simple publishing tools.

Users of social media for both business and personal purposes must comply with all relevant GWF Policies.

Mobile device/management and monitoring

GWF may install management software to all Systems and Assets to allow for remote support, security and management. As part of its monitoring and logging of Systems and Assets, GWF may:

- stop emails or messages from entering or leaving any System if it believes it is appropriate to do so; and/or
- block a User's access to Systems; and/or
- remove software, access to software, data or any other component that has been installed on an Asset or a User's asset that is being used to access GWF data, processes or networks or that is not authorised to be on that Asset/asset.

Logging and Monitoring

All actions performed using the Systems or Assets are logged and may be monitored by GWF or by another person on GWF's behalf. This includes but is not limited to document creation, file management, email or messaging sent to or by Users (internal and external), and internet activity including the sites visited, the content of those sites and the time spent at each site, mobile phone usage including call locations and durations and mobile data usage. GWF may copy, access or disclose any information or files that are stored, processed or transmitted using the Systems or on the Assets at any time.

A User should not have any expectation of privacy for any actions performed using Systems or Assets, including personal emails, instant messaging, internet access or documents, and should also be aware that these may be archived by GWF as it considers appropriate. In addition, files a User has deleted may still exist in GWF's backup systems and may be recoverable. Employees are required to retain all important information relevant to their role and the business. Employees should not rely upon BTS-IS to recover deleted items that are relevant to the business.

Email is monitored against sender/recipient and is scanned against known inappropriate content. Email quarantined for inappropriate content may be opened by IS Operations staff during their duties. Inappropriate content will be regarded as a breach of this guideline.

Internet activity is monitored including the sites visited, duration on sites and social media use. Inappropriate content is logged and alerted and may be reviewed by IS Operations staff during their duties. Inappropriate use or content will be regarded as a breach of this guideline.

GWF Reserves the right to withdraw access to any computer systems and communication services, including internet services at any time.

Line Manager Responsibility

Managers are responsible for ensuring that all existing and any new staff in their team(s) have read and understood this guideline and the GWF IS Use Policy prior to accessing GWF Assets and Systems.

Computer system access is granted so that employees can access information relevant to their own position or job function, as well as a means of communicating with colleagues and for that reason it is particularly important for line managers to ensure that staff receive appropriate training in the use of all operational computer systems and applications.

Network Access

Requests for access to the GWF Corporate Network will be processed upon submission of a request form to the IS Service Desk. An appropriate line manager must authorise each form prior to submission.

In the event of an employee leaving or no longer requiring network access, the relevant line manager must immediately advise the IS Service desk.

Network access is gained by a unique username and password. These details must NOT be disclosed to other people for their use.

Internet Access

Internet access is granted on the basis that it will be used for business related material. Limited use of internet facilities for personal purposes is permitted provided it does not interfere with the employee's performance of their role, or otherwise breach these guidelines.

GWF will not accept responsibility for theft of identity or personal data whilst conducting personal transactions such as banking, ordering goods or services etc. using GWF corporate equipment.

Any internet activity, which involves live real time entertainment i.e. live video streaming or live radio, is not permitted. The viewing of short video presentations is acceptable.

If you inadvertently accessed any type of unacceptable material or content, you should immediately report the matter to the GWFIS Service Desk who will help you delete any record of this material from your computer.

GWF reserves the right to prohibit access to certain specific internet content.

External Memory Devices

Due to the risk of loss of data/information assets external memory devices such as USB Memory Sticks, USB Disk Storage, SD Cards, MMC/XD/MS Cards should not be used for storage of any business data.

These devices are only to be used for the temporary movement of data between PC or Laptop systems and should be encrypted (must be for data classified as restricted). ALL data must be removed from these devices when they are not in use.

Alternate more secure options such as OneDrive should be considered as an alternative for file transfer. Please contact GWF IS for any assistance in using these tools or to discuss other options.

Blogging/Wikis and other forms of online discourse

GWF employees are personally responsible for their posts.
If posting to Blogs or Wikis, the following guidelines must be followed:

- Do not blog about your role at GWF or any other related matters
- Ensure that you are speaking for yourself and not on behalf of GWF or any of its group companies
- Do not publish a blog or post to a blog work related material without a suitable disclaimer
- Respect copyright, fair use and financial disclosure laws
- Do not disclose confidential or other proprietary information
- Do not cite or reference clients, partners, or supplier
- Do not use ethnic slurs, personal insults, obscenity, and show due consideration for others' privacy and for topics that may be considered objectionable or inflammatory – such as politics and religion
- Do not publish or post information that would endanger the information security of GWF or any of its group companies

Data Protection

Any company related information, which you have created or to which you have been granted access on your PC, is your responsibility to protect and remains confidential to GWF. Computer systems must not be left logged in and unattended. GWF has deployed a password protected screensaver to ensure that your terminal is locked after a short period of inactivity.

Company confidential or restricted information should not be transmitted using email or voice mail without encryption to protect its confidentiality and integrity, especially messages sent outside the company.

When an employee is due to leave the company, this should be notified at the earliest opportunity to the IS Service desk by the HR Department or relevant business unit manager so that access to all applications can be revoked at the appropriate time.

Procurement

GWF operates a "preferred supplier" policy for purchasing software, PCs, laptops, PDAs, printers and other technology based hardware. The choice of supplier is made from a scoring system that considers service, range of product and price.

Pricing from the preferred supplier will remain competitive if purchases can be monitored. For this reason, all procurement of such items must be made by IS.

Equipment purchased outside of this central procurement process including anything purchased by an individual may not have been subject to approval for use with GWF computer hardware or networks. Such equipment should NOT be connected to GWF networks, systems or assets.

Housekeeping of Email & PC Files

Users with computer equipment connected to the GWF network should ensure that all critical files are stored on network drives or OneDrive/SharePoint. This will ensure data preservation in the event of the failure of a PC or laptop.

It is the responsibility of computer and email Users to keep only relevant files and emails within GWF provided storage. Use should be made of archiving facilities to reduce the amount of data held within the email system. Please contact the Service Desk to discuss archiving options.

Emails, Messaging and Email Security

Internal and external email is provided for all those with appropriate devices e.g. laptops, desktops or smart phone.

An email or message that may seem harmless may be highly offensive to someone else. The audience of an inappropriate comment in an email may be unexpected and extremely widespread; email is neither private nor secret. It may easily be copied, forwarded, saved, intercepted, archived and may be subject to discovery in litigation.

If you receive an email or message which you think may be inappropriate report the event to your line manager, the Service Desk and then delete it immediately. Do not forward it to anyone else.

IS scan email in and out of GWF, where this type of material is found it will be quarantined within the GWF corporate email system with notification returned to the sender and GWFIS administrators.

Sensitive attachments can be protected by password protecting files or encryption. Always remember that emails may have to be disclosed to third parties irrespective of the fact that they may be confidential. Additionally, under the legal rules of disclosure, a party to the legal proceedings may be compelled by the court to deliver all documents relevant to those proceedings to the other party.

Email and Internet Good Practice

Email and internet can assist Users in performing day to day activities. The following procedures should be followed to ensure the optimum performance of email and internet usage.

- Email is not a secure method for transferring data and should not be considered private
- Contracts entered into by email may be legally binding. Speak to the legal team about the best way to enter into binding contracts. You should not use email to store contracts or other legal commitments
- Email is not a guaranteed delivery mechanism, email can be blocked by filters, scanners or simply appear as SPAM and be quarantined
- It is important that we maintain our professionalism when using electronic email, particularly with clients and customers, and apply the same standards of presentation that would apply to normal mail wherever possible
- You should take care with remarks that are or might appear to be critical of the recipient or another person. Do not assume the email will be read in context of the conversation that has happened before
- Think before sending an email – would it be more appropriate to have a face to face meeting or a telephone call
- It is advisable to state explicitly if you do not wish a message to be forwarded to others or if the information is confidential or privileged.
- Avoid sending unnecessary copies, e.g.: as a default, reply to 'sender' only, not 'all recipients' ensure the correct distribution list is selected.
- Never forward legal advice. Speak to the legal team about how this information can be shared.
- When replying to a an email, do not quote (add) the whole of the original message unless there is a reason to do so
- The sending of large files as attachments to email messages is not advisable as this creates problems transferring data over the wide area network, slowing down response times for other Users
- Use "rules" and out of office features to alert internal Users that you are away and cannot deal with their email message
- Email and other internet services should not be used for formal communications where a permanent record needs to be kept
- Commercially sensitive attachments should be password protected or encrypted to avoid unauthorised access. Regular 'housekeeping' of your inbox should be conducted. If emails do not have to be retained for business purposes they should be deleted. Personal files should also be used to free space within a User's inbox
- If you receive an email by error, you should notify the sender immediately and delete the message from your computer

- SPAM is the general term for unsolicited commercial junk email delivered across the Internet. Users should delete SPAM emails as soon as they receive them. Users should not reply to SPAM emails and should **not** click the 'unsubscribe option' To reduce the number of SPAM emails, employees should not use their GWF address on the Internet
- 'Spoofing' is a tactic that is used to mask the source of emails. The term refers to emails that appear to have originated from one source when they have been sent from another. If an employee receives a spoofed email they are advised to notify GWFIS and their line manager and delete it immediately
- Group distribution lists should only be used if there is a valid business need. Emails should not be sent to inappropriate recipients

Internet

The quality of the information on the Internet is highly variable. Users must make a judgement on the validity of the information gathered.

- Downloaded information may be subject to copyright and usage restrictions
- Do not play games on the Internet it can increase the risk of viruses and impact on performance
- Only download documents/files from trusted sources on the Internet
- If you accidentally open a site containing unauthorised material, you must immediately close it and if appropriate report it to your line manager
- Personal usage of the Internet should be kept to a minimum and should only be conducted outside of normal working hours. Excessive use of the Internet could result in disciplinary action being taken
- Business email addresses should not be published on internet newsgroups, chat rooms or social media sites, unless you have a valid business need

E-Business

As the world moves toward a virtual marketplace, increasingly business is transacted electronically. However, the very qualities that make e-business attractive also make it susceptible to increased risk, often characterised by unreliable services and lack of security.

Increasingly, businesses are using business-to-business (**B2B**) and business-to-consumer (**B2C**) transaction models to optimise their supply chains, and in many instances their entire value chains. Critical to such initiatives are the infrastructure and operational controls – also known as e-Business controls – associated with the execution and deployment of an organisation's electronic business strategy and related technology solutions.

GWF businesses engaged in B2B and/or B2C electronic transactions must ensure that satisfactory control exists and is maintained in the following areas;

- **Authenticity** (is the sender/receiver who they say they are?)
- **Confidentiality** (is the document viewable by unauthorised parties?)
- **Integrity** (can the document be altered?)
- **Non-repudiation** (sender cannot deny sending, receiver cannot deny receipt)
- **Auditability** (clear message audit trail)
- **Assured delivery** (positive confirmations)
- **Payment certainty for B2C systems** (authorisation and control of credit card transactions)

Auditing

Computer systems will regularly be audited to ensure compliance with software installation and desktop personalisation. BTS-IS personnel will carry out random checks on equipment and record this in an audit log.

Breaches of any kind will be referred to People and Performance and the line manager of the individual concerned.

Consequences of Breaching this Guideline

GWF retains discretion to commence disciplinary action for breaches of this Guideline. Disciplinary action may include a written warning, counselling, suspension or the termination of your employment or engagement. GWF may also refer a breach of this Guideline to law enforcement authorities where necessary.

Your obligations

All Users are responsible for ensuring that you are familiar with and comply with these guidelines, attend any regular training and take all reasonable steps to ensure that the workplace is free from unacceptable behaviour.

If you observe another person acting in contravention of these Guidelines, you are required to notify an appropriate member of management. All notification will be treated impartially and confidentially, except to the extent GWF may have to disclose information to a regulatory body, as required by law or to allow for a proper investigation or disciplinary process.

Related documents

- Red Book
- Code of Conduct
- Workplace Behaviour Policy
- Health & Safety Policy
- Information Systems Use Policy
- Mobile Device Management Policy
- IS Governance Policy