Information Systems Use Policy

Effective date	1st February 2022
Policy owner	BTS
Applies to	All GWF employees, contractors, customers, visitors and related entities of GWF supported by GWF IS
Contact Officer	Your Functional/Divisional People & Performance Partner
	This signed statement of Policy confirms our commitment to making GWF workplaces safe and healthy for ALL and is to be displayed at all work locations.

Purpose and aims

George Weston Foods Limited and George Weston Foods (NZ) Limited and their related companies supported by GWF IS (**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 access to inappropriate material and difficulties protecting confidential information, which we need to properly address.

This Information Systems Use Policy (Policy) addresses these issues in our workplace by providing guidance as to what is and is not an acceptable use of information systems at GWF. If you work at GWF in any capacity, including employees of GWF or employees of related entities supported by GWF IS, potential employees and contractors and on a full-time, part-time or casual basis, on or off-site, or if you are a customer or visitor attending our workplace or an event we have organised (**you**, **person**, **people**), then this Policy applies to you and you must familiarise yourself with, and comply with, this Policy and any variations to this Policy. This Policy is subject to all relevant legislation.

This Policy may be reviewed, varied, added to or withdrawn by GWF at any time, at our absolute discretion.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

Openness

GWF will make this Policy available through the Intranet or displayed at site in accordance with the applicable industrial agreement.

When does this Policy apply?

This Policy applies to all work-related situations including, but not limited to, when you are:

- in the workplace, whether during or outside normal working hours.
- during work activities, including but not limited to dealings with colleagues, clients and customers whether on or off-site, whether face to face or using information systems or media forms; and/or
- at work-related events, including but not limited to conferences and social functions.
- Accessing GWF information at any time on a personal device

Information Systems

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

- all our assets (tangible and intangible) including data, computers, telephone, electronic equipment, 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 by GWF, including our networks, remote access networks, internet, e-mail, mail storage, cloud based or any form of communication systems and IS facilitated processes such as financial, backup and recovery, availability, project design, business continuity, disaster recovery, governance, procurement, auditing and licensing (Systems)
- data and applications installed or used on **authorised** personal devices for any purpose (BYOD)

Acceptable use of IS

We provide the Assets and access to the Systems for business purposes in accordance with our policies. Acceptable use of Assets and/or Systems includes:

- communication on matters relating to your job requirements.
- communication of information relating to us or our clients, customers or suppliers.
- research on customers or clients and their businesses.
- research and information gathering that is necessary to complete job tasks

Although incidental and occasional personal and study use is permitted on GWF Assets, such use must be in accordance with our policies. We are not responsible for any personal content stored on your computer and it is your responsibility to ensure compliance with copyright, intellectual property and other applicable laws.

Access to specific applications and data may be authorised on personal devices (BYOD). Where this authorisation has been granted the device must be enrolled in the GWF Mobile Device Management service to protect the GWF data/applications. Where possible this software will be limited to GWF applications and data. Additional policy and guidelines on mobile device management can be found in the GWF Mobile Device Management Policy on the GWF Intranet)

Unacceptable use of IS

You must not use the Assets and/or Systems in breach of any of our policies. Unacceptable use of Assets and/or Systems (which also covers access external to our work sites) includes:

- for personal reasons, such that it unreasonably interferes with your performance of employment or contractual obligations.
- to conduct or facilitate the administration of personal business for commercial gain.
- for solicitation activities unrelated to our business, such as political or social campaigns.
- to access or send defamatory, threatening, discriminatory or obscene material to any persons.
- to access inappropriate material including but not limited to Pornography, Terrorism, Weapons and Internet Gambling.
- to give an unauthorised opinion of GWF.
- to send unauthorised information of GWF.
- excessive use of streaming/downloaded content.
- to use in a manner which interferes with the rights or activities of other users or our clients; and
- for any illegal or unlawful activity

There may be cases where you may, in circumstances beyond your control, receive inappropriate communications (either internally or externally). However, you should not store or further distribute (either internally or externally) such communications if received. The act of forwarding on of inappropriate material may be sufficient to breach this Policy and/or relevant legislation, even if you did not create the material.

We reserve the right to block any activities if we believe that it is necessary and permitted by law. We may block Internet sites and emails where we have reason to believe that they:

- may contain material which may breach the law or any GWF policy;
- are accessed in breach of a GWF policy;
- are spam;
- contain material which may harm the Assets and/or Systems;
- they place an unreasonable load on our Assets and/or Systems; or
- they are not apparently relevant to the acceptable use of IS as outlined in this Policy.

Security

You must not permit the use of your account by, or disclose the details of your login or password to any other person. You should create passwords that are not obvious and change your login and/or password regularly or when requested by GWF to maintain appropriate security of systems, assets and confidential information.

Monitoring of Assets and Systems

Your use of Assets and Systems is monitored for security, network maintenance and audit purposes, including for breaches of this Policy. Our monitoring activities may involve backups of emails and communications sent to or from our Assets and Systems. Additionally, activity could include performance of regular and continuous scans, logging, random or intermittent checks such as noting and recording the location of content, dates, times, material accessed and actions taken.

We (including any of our agents, nominees or any other third parties we have engaged) reserve the right to:

- monitor the use of the Systems, Data and access GWF Assets, including any personal content stored on GWF Assets[1] and/or Systems; and
- access, monitor and review the information

The IS Director (GWF) is responsible for determining who may access information obtained through that monitoring. Where a specific investigation is required, access may also be provided to P&P, Management, Legal and other personnel involved in that investigation, as well as to third parties such as legal advisors, law enforcement agencies, technology and security consultants and computer forensic specialists.

Be aware that your internet usage, emails and other information created and/or sent by you may be accessed by other users when required during business activities. All information sent and received by your company email address is our property and may be archived for possible future reference.

Routine access is available to authorised IS personnel according to the duties of their role.

Compliance with laws and policies

We require that you comply with:

- all our policies, including those regarding any aspect of workplace behaviour whether privacy management, discrimination, sexual harassment, victimisation, or bullying, or any other act in breach of company policies warranting disciplinary action.
- relevant policies of our parent company, Associated British Foods, including the Red Book and the IT Security Policies regarding the secure management of Assets, Systems and data (including documents and information); and
- any rules applicable to use and access of websites, networks or computing resources established or supplied by other entities.

[1] Where a BYOD device is in use, every effort will be made to limit monitoring and configuration to GWF Applications, Data and minimal baseline security configuration.

Your obligations

You are responsible for ensuring that you are familiar with this Policy, comply with this Policy, attend any regular training dealing with this Policy and take all reasonable steps to ensure that the workplace is free from unacceptable behaviour.

If you observe another person breaching this Policy, you are required to notify an appropriate member of management. All complaints 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.

Consequences of breaching this Policy

We retain discretion to commence disciplinary action for breaches of this Policy. Disciplinary action may include a written warning, counselling, suspension or the termination of a person's employment or engagement. We may also refer a breach of this Policy to law enforcement authorities where necessary.

Related documents

- Code of conduct
- Workplace Behaviour Policy
- Health and Safety Policy
- Information Systems Use Guidelines
- Mobile Device Management Policy

Statement from Chief Executive

I am fully committed to the implementation of this Policy and the motivation of all our people to achieve its objectives.

Stuart Grainger

GWF Chief Executive

Last Modified: February 2022