Information Systems Use Policy

Effective date	1 September 2011
Policy owner	Group Finance
Applies to	All GWF employees, contractors, customers and visitors, Australia & New Zealand
Contact Officer	Your Functional/Divisional Information Systems Partner
	This signed statement of Policy confirms our commitment to making George Weston Foods Limited workplaces professional for ALL and is to be displayed at all work locations.

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 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 acceptable use of information systems at GWF. If you are an employee, contractor or third party who makes use of IS provided by GWF (**user, you, your**), this Policy applies to you and you must familiarise yourself with, and comply with, this Policy and any variations to this Policy.

This Policy may be reviewed, varied, added to or withdrawn by GWF at any time, at our absolute discretion.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 independent contractor agreement (as the case may be).

Openness

GWF will make this Policy available through the People Portal.

Information systems

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

- all our assets 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**).

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; and
- research and information gathering that is necessary to complete job tasks.

Although incidental and occasional personal and study use is permitted, 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.

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 in connection with political campaigns;
- to access or send defamatory, threatening, discriminatory or obscene material to any persons;
- to give an unauthorised personal opinion of GWF;
- to send unauthorised confidential information of GWF;
- 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 mere 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 if it were accessed or created by a user;
- are accessed on many occasions 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 the Assets and/or Systems; or
- they are not apparently relevant to the acceptable use of IS as outlined in this Policy.

In some cases, we are obliged to provide a notice to you that an email has been blocked.

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 when requested by GWF to maintain appropriate security of our 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 breach of this Policy. Our monitoring activities may involve backups of emails and communications sent to or from our Assets and Systems and the performance of regular and continuous scans and logs or 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 use and access to Assets and/or Systems, including any personal content stored on Assets and/or Systems; and
- access the information monitored and review that information.

The Chief Information Officer is responsible for determining who may access information obtained through that monitoring. Generally, routine access will be available to authorised IS personnel. Where issues arise, access may also be provided within GWF to HR, management and other personnel involved in any investigation, as well as to third parties such as legal advisors, law enforcement agencies, technology and security consultants and computer forensic specialists.

In addition, please be aware that your emails and other information created and/or sent by you may be accessed by other users when required in the course of business activities. All emails sent and received by your company email address is our property and will be archived for possible future reference.

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 Governance Policy 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.

Your obligations

If you observe another user breaching this Policy, you are required to notify an appropriate member of management. All complaints will be treated impartially and will be addressed promptly.

Breaches of policy

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

Related documents

- Code of Conduct
- Workplace Behaviour Policy
- Health & Safety Policy
- Information Systems Use Guideline

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.

Andrew Reeves, GWF Chief Executive

Last Modified: September 2011
Published by:
Supplied by: