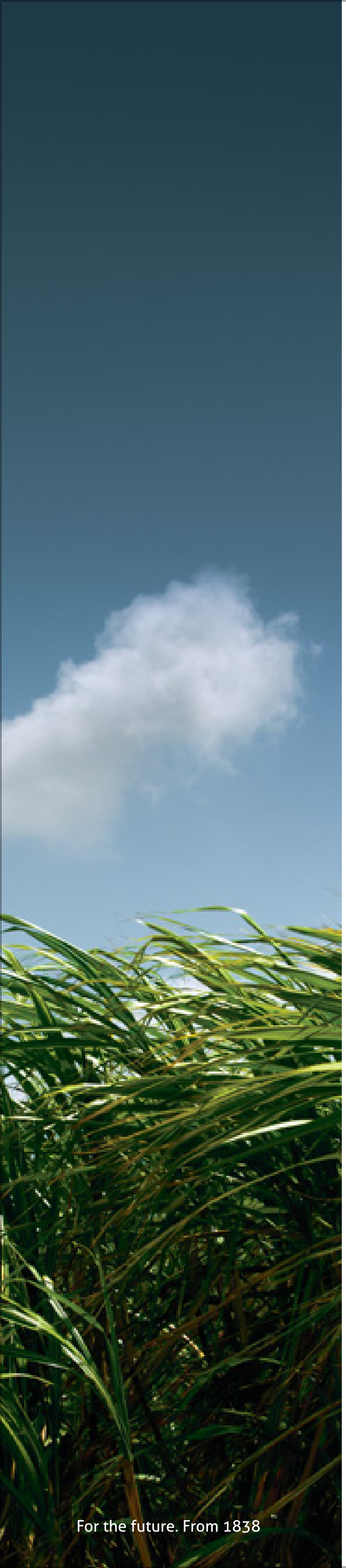
TERRA MAURICIA LTD

Information Technology Usage Policy (Version 2014 – V1.7)

For the future. From 1838

terra



For the future. From 1838

Information Technology usage policy governing the use of computers, computer services, communication devices, including e-mail and Internet

All hardware, software, applications, computing services, data, electronic files and communication devices, collectively referred to as "information systems", "systems" or "services", and which are provided to employees are considered to be the property of Terra Mauricia Ltd and its subsidiaries, referred to as "the Group".

As such, data and electronic files can be subject to review and/or monitoring, without permission of the employee. Data and electronic files include, but are not limited to, all files located on computers, servers, storage appliances and communication devices, copied or created by applications and other mediums including e-mails sent and received through the Group's e-mailing systems.

All employees who use the Group's information systems must do so in a responsible and legal manner. Moreover, all employees are responsible for maintaining the Group's integrity and reputation when using these systems.

This policy is intended to help each employee fulfil these responsibilities and may be regarded as an 'electronic code of conduct'. This document is not superseding any other code of conducts, procedures, manuals, ethical code of conduct already implemented within the Group.

The content of this 'electronic code of conduct' is non-exhaustive and may be revised as often as the Group sees fit in regard to new technological advances or other reasons.

The Group takes this matter seriously and failure to observe this policy may result in disciplinary actions.

Context

The Group encourages you, within the guidelines set out below, to explore for work purposes the potential of the electronic tools which has been provided to you. The systems and services provided by the Group are for business purposes only. You may not use them for personal gain or to express personal opinions. You must remember that when using these systems, particularly e-mail and Internet, you are representing the Group to the outside world.

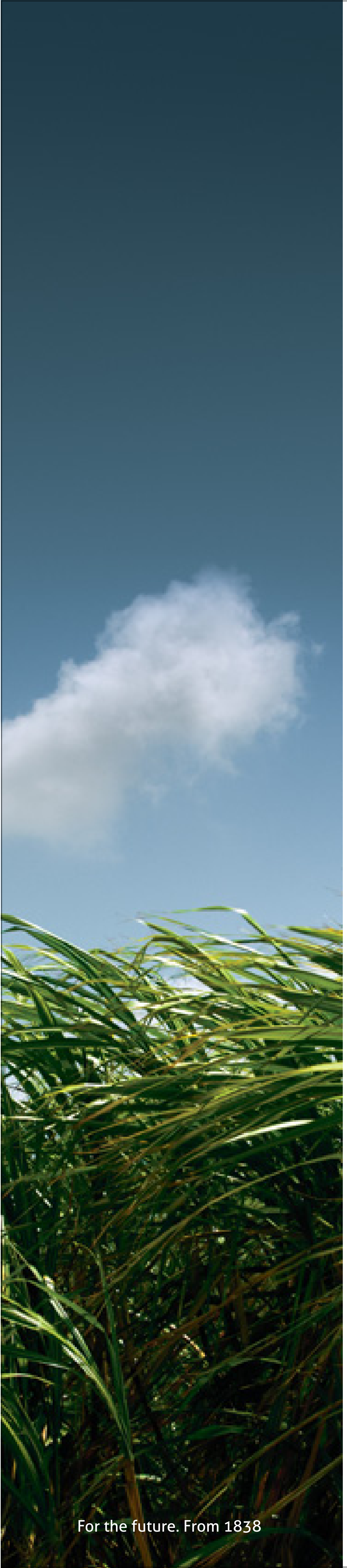
Software

Software include and is not limited to licensed software, OEM licenses, freeware, apps and open source packages. The legal requirements governing software use and distribution are complex and various. Therefore, great care must be taken, particularly when copying and installing software. Illegal copying of software is considered theft. Copyright laws govern the ownership and use of software. Infringement can lead to criminal prosecution and liability for damages.

Be aware that it is not only common programs such as Microsoft products that are controlled by licensing agreements, but also items such as fonts, templates, drivers, sound files, graphics, logos and screen savers.

Please remember it is not what you consider reasonable use of the software, but what has been agreed to, however unreasonable this may seem, in the licensing agreement governing its use. Please seek advice from the Group IT Department if in doubt.

In addition to causing the Group to be in breach of copyright law, copying of unauthorised software can also affect the integrity of the Group computer systems by introducing software that is incompatible with those systems or which might carry computer viruses or other hazards.



For the future. From 1838

To avoid these dangers:

- You are not allowed to install any software on the Group's systems. Only authorised personnel from the Group IT Department is allowed to do so.

- Do not attempt to download any software on any machine or device belonging to the Group without prior approval from the Group IT Department.

- Do not copy software from an office computer or systems to your personal home computer (or vice-versa) without the prior consent of the Group IT Department.

E-mail and Internet

The Internet is not a secure medium, and all messages created, sent, or received over e-mail and the Internet is, therefore, considered unsecured information.

The Group reserves the right to monitor or access any system and delete messages or files on any of these systems.

The Internet and other systems may not be used to access or create pornographic material. No abusive, profane or offensive material in any form (pictures, sound, text, video, e-mail, etc.) may be stored in or transmitted through any part of the Group's systems and network.

Likewise, the Group through its Group IT Department reserves the right not to grant access to specific Internet resources, which are and are not limited to, non-work related, non-productive, offensive, abusive, profane and bandwidth intensive.

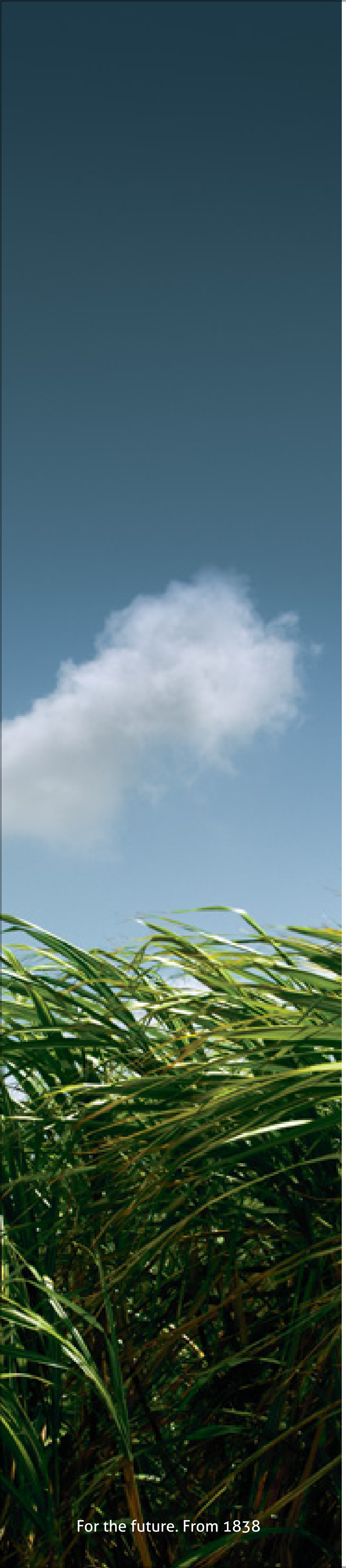
Never download software from Internet or e-mail without the permission of the Group IT Department, because you may unwittingly introduce a computer virus into the Group's systems or otherwise disrupt the stability of your computer or the entire system. Never provide access to third parties to the network, Internet connection or systems unless the Group IT Department has provided an official authorisation.

E-mails are not designed to transfer large files. It is your responsibility to ensure that the attachment file size is reasonable before sending an e-mail. If in doubt, please contact the Group IT Department. Do not send multiple e-mails with smaller attachments believing that it will be a workaround. Sending multiple e-mails with attachments to external recipients is often considered as mass-mailing and may result in the blacklisting of our domain names. Remember that companies to which an e-mail is sent have filters set and they have the right to reject emails which are considered too large.

Do not present personal opinions as being representative of the Group. E-mails are permanent written records capable of widespread publication. They can be used as evidence in court (e.g. in a libel action). Under certain jurisdictions, e-mails can be used as evidence of a contract. If in doubt, mark communications "subject to contract". Mark e-mails containing sensitive information as "confidential". Where appropriate, consider using password protection for enclosed documents. Do not read other people's e-mails without their express permission.

Immediately delete e-mails which may have reached you in error. Do not use e-mail for unauthorised mass-mailing or joining subscriber lists indiscriminately as that can put a strain on the e-mailing systems and other computer resources.

Do not use e-mail or the Internet, or any other electronic means, to engage in harassment of any kind for any reason against any group or individual. Remember that what you consider to be banter, another may consider harassment.



For the future. From 1838

Copyright

Unauthorised copying of a third party's property, including making a hard copy or electronic copy or simply storing the work without the permission of the owner, constitutes infringement of copyright. You may not freely copy works available on the Internet, Intranet or other group systems. Copying third party property may expose the Group and yourself to action for infringement, including a claim for damages.

Do not use a third party's brand or business name without prior permission. Do not take unfair advantage or use them in a manner that is detrimental to the character or reputation of that brand or name.

Do not reproduce copyrighted material without authorisation from the copyright owner.

Data storage

Only work related data and electronic files may be stored on the Group's systems. You may not use the Group's systems for storing personal photos, games, videos, downloaded software, pornography, joke material, or items of a distasteful or offensive nature. The Group reserves the right to monitor, assess or delete any files, whether maintained on the network, server or on the workstation you use.

The Group maintains a policy for backing-up data and information stored on servers; however, if data is stored on your laptop or workstation, it is your responsibility to ensure that is backedup. Please contact the Group IT Department if in doubt.

Laptops and mobile devices

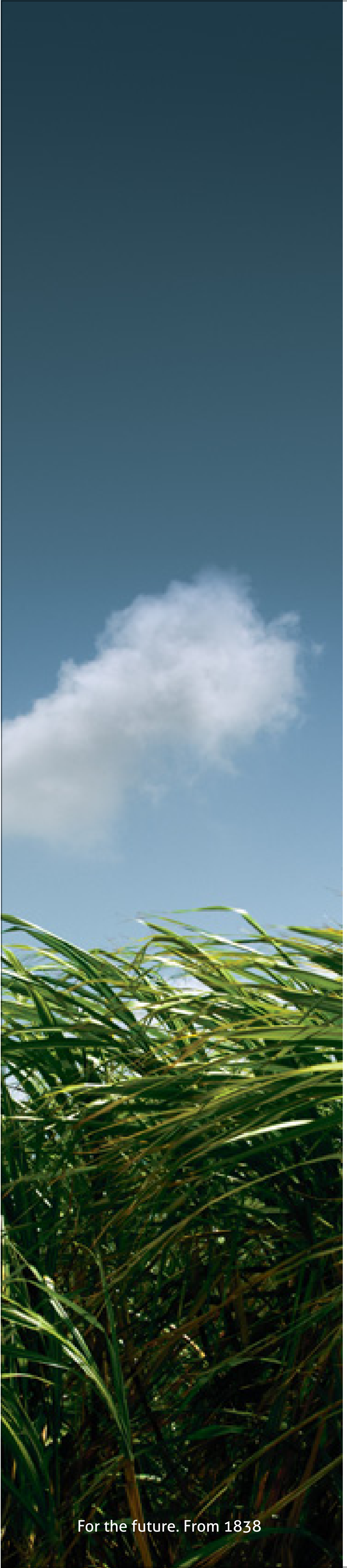
You may use the Group's property (laptops and mobile devices) outside the premises only with permission from your immediate supervisor and/or head of department. If in doubt, please contact the Group IT Department for advice.

Laptops and mobile devices must be used responsibly and kept secure at all times, particularly when left unattended. Do not forget to remove disks, flash drives and other peripherals from the laptop when not in use and store them securely. Always carry the laptop in its case to protect it from damage.

Usernames and passwords

You are responsible for your user names and passwords. Do not share your username and password and never let anyone use yours. It is your responsibility to memorise your username and passwords and do not write them down. If temporary passwords are required, make sure they are held safely until changed or cancelled. Change your password immediately if you suspect that it has been compromised. Do not use passwords that can be easily guessed.

In general, your password shall be a minimum of 6 diverse characters which should be made up from at least 3 out of the 4 different types of characters as follows: uppercase letters, lowercase letters, numbers and symbols. Do not use your name, date of birth, address or other personal data as passwords.



For the future. From 1838

Your password shall be changed frequently. The Group reserves the right to alter and enforce password policies for different applications and systems. Do not use the same passwords (or variation of the same passwords) repeatedly. Do not store your password in programs or on unprotected electronic files. Remember, you are the only employee that can gain access to your computer using your own password.

A member of the Group IT Department may require your password to intervene on your workstation. Please change the password immediately after the intervention is completed.

Viruses and other threats

A computer virus is a program designed to corrupt of destroy other programs or files. The Group has installed a corporate anti-virus software to protect our systems and workstations. You must not attempt to remove or disable this software from your computer. Do not use any unauthorised software or allow any demonstration programs to be run on your computer.

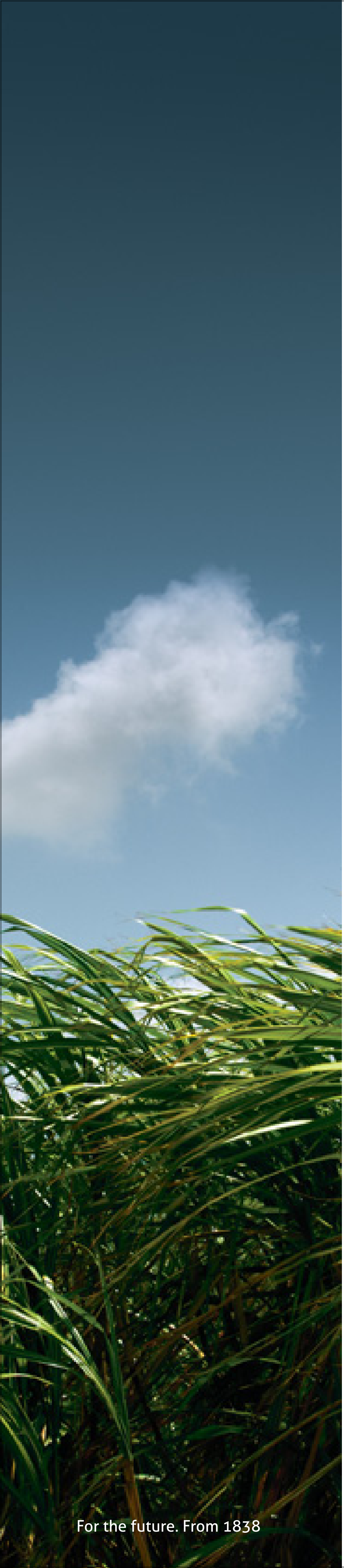
Remember, computer viruses can be exchanged between systems via different medium, including network, flash drives, optical media, external hard drives, e-mails and the Internet.

Personal use of computers

Incidental and occasional personal use of company computers is allowed for reasonable activities that do not require substantial hard disk space, network bandwidth or other computer equipment.

The above policy is intended to help you make the best use of the system and services at your disposal while allowing the Group to conduct itself in a legal, secure, and reputable manner. If you have any questions on interpreting this policy, or can point to improvements or omissions, please contact your immediate supervisor or the Group IT Department.

– o – o – o – o –



For the future. From 1838

INFORMATION TECHNOLOGY POLICY

(Version 2014 – V1.7)

Governing the use of computers, computer services, communication devices, including e-mail and Internet

I, ____, hereby acknowledge having read and understood the Information Technology Policy, governing the use of computers, computer services and communication devices, including e-mail and Internet, also referred to as ‘electronic code of conduct’, and that I agree to be bound by the terms set forth in it.

I further understand that this document cannot and shall not constitute a contract of employment.

Date: _________________

Employee’s signature: _____________________________

terra