Date 22 October 2020

Information Technology Resources Policy
Vita Life Sciences Limited
("VLS")
ABN 35 003 190 421

Contents

Information Technology Resources Policy

Vita Life Sciences Limited

1. OBJECTIVE

1.1 This policy sets out the standards of behaviour required of all users of VLS information technology resources

1.2 This policy must be complied with at all times when accessing or using VLS information technology resources. It is the responsibility of the user to ensure that they use VLS information technology resources in a professional and lawful manner.

1.3 If a user is unsure about any matter covered by this policy, they should seek the assistance of their respective Country Manager/ National Sales Manager or the Managing Director of VLS.

1.4 This policy shall be available publicly on VLS's website: www.vitalifesciences.com.au

2. SCOPE

2.1 This policy applies to members of the Board of Directors and, staff of the Company, Vita Life Sciences Ltd (VLS) together with its subsidiaries ("Company" or "Group") and, contractors (including sub-contractors and temporary contractors) ("users").

2.2 This policy applies to the use of all of VLS's information technology resources (including but not limited to internet, email and computer facilities) ("IT resources") at all hours whether in the workplace or from remote locations.

2.3 Use of computer facilities includes use of laptops, notebooks, mobile/ smart phones, TV and any other similar technological communication devices, and any other equipment that provides a means of accessing VLS email and internet facilities at any time on or off site.

3. RESOURCES

3.1 IT resources are provided solely for the business and administrative activities of VLS. These IT resources may include:

- VLS IT network (internally or externally)
- Computer systems and software which includes personal computers, notebooks and servers
- Mobile/ smart phones
- Access to the internet and/ or cloud services

- Email, phones and, other communication devices or services
- Any other devices which may be connected, linked or communicated with any or all of the above devices

4. PERSONAL USE

4.1 VLS permits users to use the IT resources for limited, incidental personal purposes, subject to the proviso that such use does not:

- Interfere with VLS business operations
- Breach this policy or any other policy and/ or code of conducts of VLS
- Negatively impact the user's work performance
- Hinder the work of other users
- Damage the reputation, image or operations of VLS
- Such use does not incur additional costs or resources to VLS

4.2 VLS expressly accepts no responsibility for:

- Loss or damage or consequential loss or damage however incurred, arising from the use of its IT resources
- Loss of data or interference with files arising from the efforts to maintain the IT resources

5. GUIDELINES FOR USE

5.1 Users must comply with the following guidelines when using the IT resources:

- Users must only use their own username/ login code and/or password.
- Users should protect their username/ login and passwords at all times and not divulge such information to any other unauthorised person, unless it is necessary to do so for legitimate business reasons
- Username/ login and passwords are not to be recorded on or near the relevant equipment/ mobile devices.
- Users should ensure that they log off from their account and, lock their computer/ mobile device or shut down their computer/mobile device when leaving such equipment unattended

5.2 Users of VLS owned computer equipment or mobile devices (including laptops, notebooks, mobile/smart phones, etc) must at all times ensure that such equipment is securely stored to minimise the possibility of theft or damage.

5.3 VLS allows reasonable personal use of IT resources and users are encouraged

to use good judgment and integrity when doing so. IT resources must not be used for private commercial purposes except where expressly sanctioned by VLS or the work is for the benefit of an entity in which VLS holds an interest

5.4 Use of proprietary software is subject to terms of license agreements between VLS and the software owner or licensor and, may be restricted in its use.

6. PHOHIBITED CONDUCT

6.1 Certain behaviour is considered to be inappropriate use of VLS IT resources and is strictly prohibited. For example (but not limited to) users must not send (or cause to be sent), upload, download, use, retrieve, or access any file, email or internet material that:

- May be deemed obscene, offensive or inappropriate. This includes text, images, sound or any other material, sent either in an email or in an attachment to an email, messages or through a link to an internet site (URL) or application, for e.g. material of a sexual nature, hateful, indecent or pornographic material
- May cause insult, offence, intimidation or humiliation by reason of harassment or discrimination
- May be defamatory or incurs liability or adversely impacts on the image of VLS. For the sake of clarity a defamatory message or material is a message or material that is insulting or lowers the reputation of a person or group of people
- Anything deemed illegal, unlawful or inappropriate
- Affects or may affect the performance of, or cause damage to or overload VLS computer systems or internal or external communications in any way.
- Gives the impression of or is representing, giving opinions or making statements of or on behalf of VLS without the express authority of VLS
- Knowingly (or should have knowingly) cause the VLS IT infrastructure to be compromised in any manner resulting in or causing (or eventually) leads to its operational failure and/ or inability to access in the usual manner

6.2 Users must not use IT resources:

- In breach of copyright or other intellectual property rights.
- To engage in any conduct that may be fraudulent.
- To engage in software, film or music piracy.
- To create any legal or contractual obligations on behalf of VLS unless expressly authorised by VLS
- That discloses any confidential information of VLS or any employee, client or supplier of VLS unless expressly authorised in writing by VLS.

- To install or run unknown or unapproved software on VLS computers. Under no circumstances should users modify the software or hardware on VLS computer systems without prior approval from the appropriate Country General Manager/ National Sales Manager.

- To gamble or engage in games of chance.

- To engage in acts for personal gain.

- Stream content for personal use.

- Use peer to peer file sharing software.

- In a manner that invades the privacy of another person

6.3 Users must not use another user's computer or internet access or email facilities (including passwords and usernames/login codes) for any reason without the express permission of the user.

7. INTERNET

7.1 VLS IT resources should only be connected to the internet using authorised means.

7.2 Users are not permitted to publish personal web pages on computers connected to the VLS network except with authorisation and approval from the appropriate Country General Manager/ National Sales Manager.

7.3 Normal and appropriate standards of civility should be used when using email and other messaging services to communicate with other staff members or any other message recipients.

7.4 When using the email or messaging system Users must not send:

- Offensive, intimidating or humiliating emails – VLS IT resources must not be used to humiliate, intimidate or offend another person/son the basis of their race, gender, or any other attribute prescribed under anti-discrimination legislation and/ or other policy or charter of VLS.

- Angry or antagonistic messages - threatening and/or bullying conduct may give rise to formal complaints and/or legal action.

8. USE OF EMAIL SYSTEM

8.1 Users must comply with the following guidelines when using VLS email system:

- Any disclaimer which is automatically included in VLS emails must not be removed.

- If a User receives an email which they suspect contains a virus, they should not open the email or any attachment to the email and should immediately contact the IT service desk for assistance.

- If a User receives an email the content of which (including an image, text, materials or software) is in breach of this policy or any VLS other policies, the User should immediately delete the email and report the matter to the Country General Manager/National Sales Manager. The User must not forward the email to any other person.

- Users must not forward or copy emails that contain personal information about an individual without the prior permission of that individual.

- Messaging and email must not be used for private commercial purposes except where the work is for the purposes of a corporate entity in which Vita Life holds an interest.

- Users must adhere to the guidelines and prohibitions set out in this policy at all times.

9. SOCIAL MEDIA

9.1 VLS IT resources are provided for work purposes only. Access to social networking websites (such as but not limited to Twitter, Facebook and other similar sites) may not be a requirement in many positions or job functions. However, if a User at the discretion of its supervisor is permitted to access social networking websites or for work related purposes, the User is responsible for ensuring that their access does not:

- Interfere with the business operations of VLS

- Violate this policy or any other policy of VLS

- Negatively impact upon the User's work performance.

- Hinder the work of other Users.

- Cause damage to the reputation, image or operations of VLS

9.2 Users must take a common sense approach to the content that they publish online.

9.3 If a User holds himself out as a representative of VLS, any material published online must:

- Be relevant to the User's area of expertise

- Not be anonymous

- Maintain professionalism, honesty and respect

9.4 Users must not publish any material online that contains VLS confidential information, the personal information of another (without that individual's consent), information about VLS customers, clients or competitors, or content that may offend, intimidate, defame or humiliate a staff member or contractor of VLS.

9.5 If a User becomes aware of the publication of material that is linked to VLS, a

staff member or contractor or VLS's clients which would be deemed distasteful or inappropriate, the User should immediately report such conduct to the respective Country Manager/ National Sales Manager or the Managing Director of VLS.

9.6 If a User is unsure about whether they should publish any material on the internet, they should seek guidance from their Country Manager/ National Sales Manager or the Managing Director of VLS.

10. MONITORING

10.1 VLS reserves the right to access and monitor any computer or other electronic device connected to VLS's network.

10.2 Access to and monitoring of equipment is permitted for any reason, including but not limited to, suspected breaches of this policy by a User or unlawful activities. Access to and monitoring includes, but is not limited to, email, web sites, server logs, application software and electronic files.

11. BREACH OF POLICY

11.1 If VLS suspects or finds evidence of a breach of this policy, VLS reserves the right to restrict a User's access to its IT resources.

11.2 Any User found to have violated this policy may be subject to disciplinary action.

11.3 All criminal offences will be reported to the police and/ or other relevant authorities.

12. CHANGES TO POLICY

12.1 The Board will review this Policy from time to time to ensure that it remains consistent with the Board's objectives and current best practice. The Company Secretary will communicate any amendments to the policy to directors and employees.