CYBERSAFETY USE AGREEMENT

Last Updated: 21st November 2018

This document is comprised of a cover page and two sections:

Section A – Cybersafety in the Work Environment
- Part 1: Important cybersafety initiatives
- Part 2: Cybersafety use agreement rules and responsibilities
- Part 3: Scope of DNA Electrical staff cybersafety use agreement

Section B – The Staff Cybersafety Use Agreement Form

Instructions for staff:

1. Please read Section A carefully.
2. If any clarification is required, it should be discussed with your Manager, before the document is signed.
3. Detach the Section B form, sign and return it to your Manager.
4. It is important to retain the remaining pages for future reference.

Important terms used in this document:

*(a) The abbreviation **'ICT'** in this document refers to the term 'Information and Communication Technologies'.*

*(b) **'Cybersafety'** refers to the safe and responsible use of the internet and ICT equipment/devices, including mobile phones.*

*(c) **'The DNA Electrical's ICT'** refers to our computer network, internet access facilities, computers, and other ICT equipment/devices as outlined in (d) below.*

*(d) The term **'ICT equipment/devices'** used in this document, includes but is not limited to, computers (such as desktops, laptops, tablets, PDAs), game consoles, storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/receivers (such as portable CD and DVD players), tablets/iPads, and any other, similar, technologies as they come into use.*

SECTION A – CYBERSAFETY IN THE WORK ENVIRONMENT

IMPORTANT DNA ELECTRICAL CYBERSAFETY INITIATIVES

This document outlines important **DNA Electrical** initiatives to help ensure the cybersafety of the work environment. We are committed to maintaining the highest standards of professional behaviour, and a work environment which is physically and emotionally safe.

This use agreement is to be read in conjunction with the DNA Electrical Employment Contract, and the Health and Safety policy of **DNA Electrical**.

Our cybersafety use agreement defines obligations, responsibilities, and the nature of possible consequences associated with breaches of the use agreement deemed to undermine the safety and professionalism of the work environment, and/or necessitate referral to law enforcement.

1. Cybersafety use agreements

1.1. All staff, *whether or not* they currently make use of the computer network, will be issued with this staff use agreement. You are required to read these pages carefully, and return the signed use agreement form in Section B to your Manager.

1.2 All ICT equipment use including use of privately-owned/leased equipment/devices on the work site, or at any work-related activity must be appropriate to the work environment.

1.3. The use of ICT equipment in any way that is inappropriate in the work environment is considered a serious matter.

1.4. Staff accept liability for inappropriate or objectionable (illegal) material they download or copy using **DNA Electrical** ICT resources. This includes objectionable[1] (illegal) content and material breaching copyright.

2. Monitoring and system audits

2.3. **DNA Electrical** reserves the right to employ an electronic access monitoring system to record internet use, including the user details, time, date, sites visited, length of time viewed and from which computer or device.

2.4. **DNA Electrical** will from time to time conduct an internal audit of its computer network, internet access facilities, computers and other ICT equipment/devices, or may commission an independent audit. If deemed necessary, auditing of the computer system will include any stored content, and all aspects of its use, including email. An audit may also include any ICT equipment/devices provided or subsidised by/through **DNA Electrical** or subsidised by a related source.

2.5. Employee exit procedures include an audit of **DNA Electrical's** ICT equipment/devices which have been used by the employee.

3. DNA Electrical response to breaches of the use agreement

3.3. A breach of cybersafety rules which is deemed to be harmful to the safety of **DNA Electrical** could result in serious consequences and may include disciplinary action.

3.4. If there is a suspected breach of the use agreement involving privately owned ICT on **DNA Electrical's** work site or at a work-related activity, the matter may be investigated by **DNA Electrical**. **DNA Electrical** may request permission to audit the relevant equipment/device(s) as part of its investigation into the alleged incident.

3.5. In the event that staff are suspected of involvement with material which is deemed objectionable (illegal), under the Films, Videos and Publications Classification Act 1993, or involvement in an activity which might constitute criminal misconduct, **DNA Electrical** may involve law enforcement agencies in addition to any disciplinary response.

3.6 Any investigation undertaken by **DNA Electrical** will include provision to the employee, or employees, who may be involved in the suspected breach of the use agreement, of an opportunity to explain his/her actions or behaviour. Fair, unbiased consideration will be given to his/her explanation.

[1] Objectionable material is defined by the Films, Videos and Publications Classification Act 1993

DNA ELECTRICAL STAFF CYBERSAFETY USE AGREEMENT RULES AND RESPONSIBILITIES

These rules have been developed to support the important cybersafety initiatives outlined in Part 1.

4. Staff are required to sign the DNA Electrical staff cybersafety use agreement

4.1. Please sign the last page of this use agreement and return it to Andrea Hoareau.

NB The entire document should be kept for reference, including a copy of the signed form.

5. Appropriate use of the internet and ICT devices as a DNA Electrical employee

5.1. **DNA Electrical** provides ICT equipment/devices for work-related activities. The amount of time spent on non work-related usage should be reasonable and not interfere with normal work duties.

5.2. Any staff member who allows another person (who does not have a signed use agreement with **DNA Electrical**) to use internet facilities or **DNA Electrical** ICT, is responsible for that use, and may be held responsible for any misuse.

5.3. Use of privately-owned/leased ICT equipment/devices (including mobile phones) on the work site, or at any work-related activity must be appropriate to the **DNA Electrical** environment.

5.4. When using **DNA Electrical** ICT at any time, or privately-owned ICT on the work site or at any work-related activity, users must not initiate access to, save, copy, show to others or print inappropriate or objectionable (illegal) material or activities.

5.5. Under no circumstances should **DNA Electrical** ICT be used to deliberately facilitate any illegal or inappropriate workplace behaviour.

6. Individual password logons (user accounts)

6.1. It is important that passwords used on **DNA Electrical** devices are strong. Passwords must use a combination of upper- and lower-case letters, numbers and symbols, and be a minimum of 8 characters in length.

6.2. Passwords and PIN codes must be kept confidential and not shared with anyone else.

6.3. Users should not allow any other person access to any equipment/device logged in under their own user account, unless as part of authorised work.

7. Appropriate use of email and communications technologies.

7.1. Electronic communication (e.g. email) must be used in a responsible manner and in accordance with this use agreement. This ensures that no electronic communication could cause offence to others or harass or harm them, put the owner of the user account at potential risk, or in any other way be inappropriate in the **DNA Electrical** work environment.

7.2. Staff must verify the contact details of recipients before sending confidential and/or sensitive information.

8. Care of ICT equipment/devices

8.1. All **DNA Electrical** ICT equipment/devices should be cared for in a responsible manner.

8.2. Any damage, loss or theft of ICT equipment/devices, or attempt to breach the security of the network must be reported immediately to your Manager or the HR Manager.

8.3. Where negligence on the part of the Employee allows damage to or loss of the property of the Employer in the care of the Employee, the Employee shall as directed by the Employer be required to either replace property that is damaged or lost or reimburse the Employer for such damage of loss.

8.3.1. For clarification it is expected that staff shall keep any ICT equipment/devices they have been issued stored securely and safely, not able to be accessed by anyone other than DNA Electrical staff. For illustration, when stored in a vehicle the device must be kept “out of sight” at all times. Storing or keeping ICT equipment/devices where they are visible in a vehicle or in a location where they can be visually seen or accessed by anyone other than DNA Electrical staff shall be seen as negligence on the part of the employee

9. Wastage

9.1. All users are expected to practise sensible use to limit wastage of computer resources and/or bandwidth. This includes avoiding unnecessary printing, and unnecessary internet access, uploads or downloads.

10. Installing software and connecting hardware

10.1. Users must not download, install or connect any software or hardware onto **DNA Electrical** ICT equipment/devices, or utilise such software/hardware without prior authorisation. This includes use of such technologies as Bluetooth, infrared, wireless, and any other similar technologies which may be developed.

11. Copyright and licensing

11.1. Copyright laws and licensing agreements must be respected. This means no involvement in activities such as illegally copying material in any format, copying software, downloading copyrighted video or audio files, using material accessed on the internet in order to plagiarise, or illegally using unlicensed products.

12. Posting material

12.1. All material and links published on **DNA Electrical** internet/intranet/social media should be appropriate to the **DNA Electrical** work environment.

12.2. Such material can be posted only by those given the authority to do so by the **DNA Electrical**.

12.3. No employee may bring **DNA Electrical** into disrepute on any website or social media platform

13. Actions to take in response to accidental access to inappropriate or illegal content

13.1. Staff must immediately notify Andrea Hoareau of all incidents, which will be recorded (including site accessed) in the ICT Incident Register by Andrea Hoareau.

SCOPE OF DNA ELECTRICAL STAFF CYBERSAFETY USE AGREEMENT

14. This staff use agreement applies to

14.1 All staff whether part-time, full-time or temporary, whether or not they currently make use of the network, internet access facilities, computers and other **DNA Electrical** ICT equipment/devices

14.2 Volunteers working in the organisation.

SECTION B - STAFF CYBERSAFETY USE AGREEMENT FORM

Please complete, sign, and date this Staff Cybersafety Use Agreement Form which confirms your agreement to follow the obligations and responsibilities outlined in this document.

If you have any queries about the agreement, you are encouraged to discuss them with Andrea Hoareau, before you sign.

Once signed, this form should be returned to your Manager for filing with staff records.

A copy of the signed form will be supplied to you.

USE AGREEMENT

I have read and am aware of the obligations and responsibilities outlined in this DNA Electrical Staff Cybersafety Use Agreement document, a copy of which I have been provided with and advised to retain for reference. These obligations and responsibilities, which I agree to follow, relate to the cybersafety of the DNA Electrical work environment and network activities. I also understand that apparent breaches of this Staff Cybersafety Use Agreement will be investigated by the IT Manager and could result in disciplinary action, and where necessary, referral to law enforcement.

Employee

Name: _____ Role: _____

Signature: _____ Date: _____

Employer

Name: _____ Role: _____

Signature: _____ Date: _____