

PURPOSE	1	Norwood recognises the usefulness of the internet, email, mobile devices and computer equipment as research, communication and work tools. This policy sets out the appropriate standards of behaviour for users of Norwood's information technology resources.
INTRODUCTION	2	At all times when accessing or using Norwood's information technology resources, users must ensure that they comply with this policy. It is the user's responsibility to ensure that they use Norwood's information technology resources in a lawful and professional manner. This policy outlines the expectations in the use of Norwood's information technology resources in a lawful and professional manner. 3.1 Information technology resources. 3.2 Internet. 3.3 Social media. 3.4 Email. 3.5 Mobile phones and mobile devices. If a user is unsure about any matter covered by this policy, they should seek the assistance of the IT Manager or Managing Director.
SCOPE	2.1	This policy applies to all staff members of Norwood and contractors (including sub-contractors and temporary contractors) referred to as users. This policy applies to the use of all internet, email and computer facilities, both during and outside of business working hours. This policy applies to the use of internet, email and computer facilities inside the workplace, as well as use from remote locations. Use of computer facilities includes use of laptops, mobile phones and similar products, and any other equipment that provides a means of accessing Norwood's email and internet facilities. For example, this policy extends to the use of a personal computer which has access to Norwood's IT systems.
BODY POLICY	3	
INFORMATION TECHNOLOGY RESOURCES	3.1	Norwood's information technology resources ("IT resources") are provided to support the business and administrative activities of Norwood. These resources include: - Norwood's network. - Computer systems and software including personal computers, notebooks and servers. - Mobile phones, smart phones and wireless data cards. - Access to the internet. - Email, telephones and related services. If users produce, collect and/or process Norwood related information in the course of their work, that information remains the property of Norwood. This includes information stored on third party websites.
EXTENT OF EXTERNAL USE	3.1.1	Users are permitted to use Norwood's IT resources outside of normal working hours for limited, incidental personal purposes, provided that such use does not: - Interfere with the efficient business operations of Norwood. - Violate this policy or any other policy of Norwood. - Negatively impact upon the user's work performance. - Hinder the work of other users. - Damage the reputation, image or operations of Norwood. - Such use must not cause noticeable additional cost to Norwood. - Norwood accepts no responsibility for: - Loss or damage or consequential loss or damage, arising from personal use of its IT resources. - Loss of data or interference with personal files arising from the efforts to maintain the IT resources.
GUIDELINES FOR USE OF IT RESOURCES	3.1.2	Users must comply with the following guidelines when using Norwood's IT resources: - Users must use their own username/login code and/or password when accessing Norwood's computer systems. - Users should protect their username/login code and password information at all times and not divulge such information to any other person, unless it is necessary to do so for legitimate business reasons. - Username/login codes and passwords are not to be recorded on or near computer 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 to ensure that others do not have access to Norwood's computer systems. - Users in possession of Norwood's computer equipment or mobile devices (including laptops, mobile phones, pagers, personal data assistants, wireless data cards, etc) must at all times ensure that such equipment is stored or placed in areas with a minimal possibility of theft or damage. - Use of proprietary software is subject to terms of license agreements between Norwood and the software owner or licensor, and may be restricted in its use.
PROHIBITED CONDUCT	3.1.3	Certain behaviour is considered to be inappropriate use of Norwood's IT resources and is strictly prohibited. Examples of such prohibited conduct are, but are not limited to: a) Users must not send (or cause to be sent), upload, download, use, retrieve, or access any file, email or internet material that: I. Is 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, or through a link to an internet site (URL). For example, material of a sexual nature, hateful, indecent or pornographic material. II. Causes insult, offence, intimidation or humiliation by reason of unlawful harassment or discrimination. III. Is defamatory or incurs liability or adversely impacts on the image of Norwood. A defamatory message or material is a message or material that is insulting or lowers the reputation of a person or group of people. IV. Is otherwise illegal, unlawful or inappropriate. V. Affects or may affect the performance of, or cause damage to or overload Norwood's computer systems or internal or external communications in any way.

- VI. Gives the impression of or is representing, giving opinions or making statements of on behalf of Norwood without the express authority of Norwood.
- b) Users must not use IT resources to:
 - I. Violate copyright or other intellectual property rights. Computer software that is protected by copyright is not to be copied from, or into, or by using Norwood's computing facilities, except as permitted by law or by contract with the owner of the copyright. Similarly, users should not copy or access copyright protected music or videos on Norwood's IT resources.
 - II. Breach an individual's privacy.
 - III. Create any legal or contractual obligations on behalf of Norwood unless expressly authorised by Norwood.
 - IV. Disclose any confidential information of Norwood or any employee, client or supplier of Norwood unless expressly authorised by Norwood.
 - V. Install software or run unknown or unapproved programs on Norwood's computers. Under no circumstances should users modify the software or hardware environments on Norwood's computer systems (this includes installing software purchased by users for personal private use) without prior approval from the IT Manager.
 - VI. Gain unauthorised access (hacking) into any other computer within Norwood or outside Norwood or attempt to deprive other users of access to or use of any Norwood computing system.
 - VII. Deliberately send or cause to be sent chain or spam emails in any format.
 - VIII. Obtain personal gain. For example, running a personal business using Norwood's computers.
 - IX. Gamble.
 - X. Stream content for personal use.
 - XI. Use peer to peer file sharing software such as VUZE, BitTorrent, etc.
 - XII. Download, install or use instant messaging software.
 - XIII. Perpetrate any form of fraud or software, film or music piracy.
- c) 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.

INTERNET **3.2** Norwood's IT resources should only be connected to the internet using means authorised by the IT Manager. Users are not permitted to publish personal web pages on computers connected to the Norwood network.

SOCIAL MEDIA **3.3** Norwood's IT resources are provided for work purposes. Access to social networking websites during working hours will therefore only be allowed for Norwood related purposes. If a user is permitted to access social networking websites, the user is responsible for ensuring that their access does not:

- Interfere with the efficient business operations of Norwood.
- Violate this policy or any other policy of Norwood.
- Negatively impact upon the user's work performance.
- Hinder the work of other users.
- Damage the reputation, image or operations of Norwood.

For the sake of clarity, social media includes, but is not limited to:

- Social networks (such as Facebook and MySpace).
- Blogs.
- Wikis (such as Wikipedia).
- Podcasts.
- Forums.
- Content communities (such as YouTube and Flickr).
- Microblogs (such as Twitter).

Users must take a common sense approach to the content that they publish online. Because of the public nature of the internet and social media, this common sense approach also applies to use of social networking sites outside of business hours or on equipment other than Norwood equipment.

If a user is holding themselves out as a representative of Norwood, any material published online must:

- Be relevant to the user's area of expertise.
- Not be anonymous.
- Maintain professionalism, honesty and respect.

Statements of fact about Norwood and its products and services, publicly available information and information already published on Norwood's website are all examples of appropriate online content.

Users must not publish any material online that contains Norwood's confidential information (including financial information and information about organisational matters), the personal information of another (without that individual's consent), information about Norwood's customers or clients, or content that may offend, intimidate, defame or humiliate a staff member, volunteer or contractor of Norwood.

Further, if a user becomes aware of the publication of material that is linked to Norwood, its workers or its clients which would be deemed distasteful or inappropriate, the user should report such conduct to the Managing Director.

If a user is unsure about whether they should publish material on the internet, they should seek guidance from the IT Manager or Managing Director.

EMAIL **3.4** 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. When using the email or messaging system users must not send:

- Angry or antagonistic messages – these can be perceived as bullying or threatening and may give rise to formal complaints under grievance procedures or discrimination/sexual harassment procedures.
- Offensive, intimidating or humiliating emails – Norwood's IT resources must not be used to humiliate, intimidate or offend another person/s on the basis of their race, gender, or any other attribute prescribed under anti-discrimination legislation.

GUIDELINES FOR USE OF NORWOOD'S EMAIL SYSTEM	3.4.1 A user must comply with the following guidelines when using Norwood's email system: - Any disclaimer which is automatically included in Norwood's 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. - <u>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 Norwood's other policies, the user should immediately delete the email and report the matter to the IT Manager or Managing Director. The user must not forward the email to any other person.</u> - Users must adhere to the guidelines and prohibitions set out in this policy at all times.
MOBILE PHONES AND MOBILE DEVICES	3.5 Users must comply with the following guidelines when using Norwood's mobile phones and mobile devices: - Users must maintain the operational effectiveness of the mobile phone or mobile device (i.e. keeping the batteries charged when required to be contacted). - Mobile phones and mobile devices that have the ability to be password protected and encrypted must have this security feature activated at all times. Users are not to remove or modify such security features when configured by the IT Department. - International and premium number call facilities will not be available without prior agreement for both business and private use. - Users must report any loss, theft, damage or security breach of any mobile phone or mobile device immediately to the IT Department to ensure appropriate measures are taken to secure and disable the device. If such loss, theft or damage is due to the negligence of the user, the user may be responsible for the cost of replacing or repairing the mobile device.
MONITORING – EMAIL, FILES, INTERNET DOWNLOADS OR DATA STORAGE	4 Norwood monitors email, files, internet downloads or data stored on its IT resources and reserves the right to access and monitor any computer or other electronic device connected to Norwood's network. This includes equipment owned by Norwood and personal computing equipment (for example, laptops) that are connected to the network. 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 and electronic files. Norwood may keep a record of any monitoring or investigations.
BREACH OF THIS POLICY	5 Where Norwood suspects or finds evidence of a breach of this policy, Norwood reserves the right to restrict or remove a user's access to its IT resources. Any user found to have violated this policy will be subject to disciplinary action including the possibility of termination of your contract of employment. Criminal offences will be reported to the police.
CONCERNS OR COMMENTS	6 If you have any concerns about the internet, email and computer use policy please contact the IT Manager or Managing Director. Resolution of concerns will be sought as promptly as possible.
CHANGES TO NORWOOD'S INTERNET, EMAIL AND COMPUTER USE POLICY	7 Norwood may modify or amend this policy at any time and an updated policy will be distributed to all relevant staff.
FURTHER INFORMATION AND ASSISTANCE	8 Adherence to this policy will generally ensure compliance with the requirements of Norwood and legislation. However, there may be instances where inadvertent breaches could occur. When in doubt users requiring assistance with interpretation of the policy, or who wish to report a breach of this policy, should contact the IT Manager or Managing Director.

Norwood Industries PTY LTD.

Fran Coyle
Managing Director

February 2016



INTERNET, EMAIL & COMPUTER USE POLICY

Attached is the revised Policy of Norwood Industries Pty Ltd, your employer:

Internet, Email and Computer Use Policy

Please read this Policy very carefully, then sign and return this form to Pauline by Friday 26 February 2016.

I confirm that I have read and understood the above Policy.

THIS AGREEMENT is made the day _____ of _____ 20 ____

Employee Print Name:

Employee Signature: