

What is the Purpose?

The purpose of this policy is to manage the use of Internet resources at Northcott sites, including customer homes.

Who needs to know about this Policy?

- This policy applies to all users of Northcott Internet resources – including (but not limited to):
 - Employees (including casuals, temp agency staff and volunteers)
 - Customers
 - Students
 - Consultants and contractors
 - Third parties
 - Visitors to Northcott.

What is Northcott's policy?

- ✓ Use of the Internet is allowed and encouraged to support customers, research, business purposes and supporting the goals and values of Northcott.
- ✓ Customers not following this policy will be managed in line with the My Service Agreement.
- ✓ **All users, including customers, their families and friends** cannot use the internet for the following activities:
 - Illegal activities. Illegal activities include:
 - Making inappropriate contact with a child or minor or providing them unrestricted access to age restricted material.
 - Any cyber attacks.
 - Making fake offers to sell or buy products, items, or services.
 - Sending or posting any material or being involved in activities which could offend, threaten or harass someone.
 - Accessing, storing, copying, sending or giving out, publishing or commercially exploiting any information or material that does not follow copyright, patent, trade mark, design or other intellectual property rights.
 - To advance a financial scam such as pyramid schemes or Ponzi schemes.
 - Use of Northcott owned domain names to conduct business other than official business.

Subject Matter Expert: Chief Information Officer		Version: 0.2
Issue Date: 14 January 2021	Next Review Date: 14 January 2024	Page 1 of 3

- In any way which damages or interferes (or threatens to damage or interfere) with the operation of a Service or how well Northcott's network or a vendors network and services work.
 - To be involved in any unreasonable activity that stops or slows down other people or systems to use Northcott's services or the Internet.
 - In a way which makes it unsafe or which may damage property.
 - To abuse, harass or undermine our staff or other customers.
- ✓ **Employees, students, consultants, contractors, third parties, temp agency staff and visitors** also cannot use the internet for the following activities (you need to follow the activities for all users as well):
- Visiting websites that have objectionable or criminal material, for example (but not limited to), pornography. This is only allowed with an email from a Level 2 Manager or Level 1 Manager stating the reason and approval to visit the websites.
 - Personal use of the internet is allowed where it doesn't negatively impact or affect your day to day role or duties.
 - Uploading or downloading commercial software, games, or music videos unless it is related to the user's work or supporting customers of Northcott.
 - Sending or receiving copyright information, trade secrets or any other private, confidential or sensitive information. This is only allowed with written approval from the relevant Northcott Executive.

Northcott's Right to view internet traffic and history

- We monitor internet traffic and view internet traffic history on our systems to make sure the services we provide are used appropriately.
- We record internet usage or internet browsing of users to make sure they are following this policy, applicable laws and industry regulations or where we reasonably think activities may not be following this policy.
- Details of an individual's internet usage can be viewed when requested by a Northcott Executive (or authorised representative) and with written approval of the CEO or General Manager People and Culture.

What other Northcott documents are related?

You may need to refer to these documents for more information:

[Information Communication and Technology Resource Use Policy](#)

[Privacy Policy](#)

[Subpoena Policy and Procedure](#)

Subject Matter Expert: Chief Information Officer		Version: 0.2
Issue Date: 14 January 2021	Next Review Date: 14 January 2024	Page 2 of 3

Who is Responsible?	What are they Responsible for?
Chief Executive	<ul style="list-style-type: none"> Final review and approval of this policy.
Level 2 Manager	<ul style="list-style-type: none"> Maintain this policy, its related procedures and documents.
Level 3 and 4 Manager	<ul style="list-style-type: none"> Ensure the policy is effectively implemented in their services. Ensure staff follow the policy.
Supervisor	<ul style="list-style-type: none"> Ensure staff have read and understand the policy and have sufficient skills, knowledge and ability to meet the requirements.
All Employees	<ul style="list-style-type: none"> Follow the requirements of the policy.

Definitions, Legislation & Standards Compliance

Definitions:

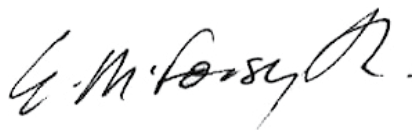
Cyber Attacks: This is where you access or try to access, monitor, use or control someone else's account or private information (including usernames and passwords), equipment, systems, networks or data. Cyber attacks include Phishing / targeted malicious e-mails, website defacement, email addresses or website(s) blacklisted, unauthorised access to information by an external user, unauthorised modification of information, denial of service attack, data loss / theft of confidential information, theft of laptops or mobile devices, unauthorised access to information by internal user, data breach and third party provider / supplier, brute force attack, crypto-mining malware, accidental disclosure, ransomware, business email compromise, payment redirection fraud, malware / trojan infections.

For other Definitions, please refer to the dictionary on the Northcott Intranet.

Legislation:

This policy and procedure was developed in accordance with the National Disability Insurance Scheme (Provider Registration and Practice Standards) Rules 2018.

For other Legislation and Standards Compliance, refer to Service Management Policy.



Authorised by:

Liz Forsyth, Chief Executive Officer

Subject Matter Expert: Chief Information Officer		Version: 0.2
Issue Date: 14 January 2021	Next Review Date: 14 January 2024	Page 3 of 3