INFORMATION TECHNOLOGY USAGE POLICY

The Oaktree Foundation Australia

Approved Date 25 March 2017	**Approved By** The Board
Next Review Date 25 March 2019	**Policy Owner** Legal Team

1. Scope of this policy

This Policy applies to all Representatives of The Oaktree Foundation Australia (**Oaktree**).

All Representatives are required to read and acknowledge the Information Technology Usage Policy as a condition of using the IT supplied by Oaktree.

2. Policy objectives

Oaktree provides Representatives with access to IT for purposes related to their role at Oaktree. The objective of this Policy is to provide a clear statement of acceptable IT use for all Representatives who use IT that is supplied by Oaktree.

3. Definitions

Approved Parties means someone who has been given permission to access Oaktree information by an Oaktree Representative who is accountable/owns that information.

Confidential information means all information concerning Oaktree which Representatives become aware of or generate including, but not limited to:

a) trade secrets; confidential know-how; personal information of Representatives; information concerning the business, finances, campaigns, research and development, marketing information, strategy or Representatives of Oaktree or any related body corporate;

b) any information that is marked, or is stated to be confidential;

c) any information which would reasonably be regarded as confidential; and

which is not otherwise in the public domain other than as a consequence of an unauthorised disclosure.

Cyber security includes all the measures taken to protect networks, computers and data from attack, damage or unauthorised access or use.

Cyber-attack describes any attempted or actual incident that either:

a) Uses computer technology or networks to commit or facilitate the commission of traditional crimes, such as fraud and forgery - for example, identity or data theft (computer assisted) or
b) Is directed at computers and computer systems or other information communication technologies - for example, hacking or denial of services (computer integrity)

Information Technology (IT) means any technology system (e.g. emails, remote access and internet access) used to store, retrieve, access, send or receive information that is supplied by Oaktree. Where Oaktree email accounts are accessed or used on a mobile internet device, the IT is considered to be supplied by Oaktree.

Internet means Oaktree-provided access to the web such as the Oaktree Wi-Fi or any other network provided by Oaktree.

IT Facilities includes any digital account or program that is used in relation to their Oaktree role such as: Oaktree email, Dropbox, Google Drive, NationBuilder, Oaktree's social media pages, and other online documents.

Representatives means Board members, Sub-Committee members, Advisory Board members, employees, contractors, volunteers, Community Leaders and anyone else performing functions for Oaktree.

4. Internet and email use

It is the responsibility of each Representative to ensure that Internet and email access is used in a responsible and professional manner. Oaktree's Internet may only be used for personal use where this use is both limited and reasonable. Any personal use of Oaktree's IT Facilities must not interfere with the performance of a Representative's duties and responsibilities. Excessive personal use will constitute a breach of this Policy.

5. Social media

5.1 Representative's Personal Social Media

Accessing social media sites for reasonable personal use while in the Oaktree office is permitted. However, excessive or inappropriate use of social media on IT supplied by

Oaktree will constitute a breach of this Policy and is grounds for disciplinary action. Inappropriate use may include, but is not limited to:

a) conduct which is inconsistent or interferes with the Representative's duties; or

b) conduct which has the potential to bring Oaktree into disrepute including, but not limited to, making comments on social media about Oaktree or other Representatives that have the potential to damage the reputation of Oaktree.

Representatives may post on their own social media regarding Oaktree where their posts are in accordance with Oaktree's values. Oaktree Representatives understand that their obligations with respect to Oaktree's confidential information and privacy continue to apply to their use of social media outside of working hours. Where Oaktree deems a post inappropriate, Oaktree holds the right to:

a) request a Representative to remove association with Oaktree on social media, including any posts or comments made about Oaktree on a personal social media account.

b) request a Representative to remove the relevant post/s or comment/s

c) terminate a Representative's relationship with Oaktree, if they refuse to do the above and/or where the offence is deemed serious

5.2 Oaktree's Social Media

Oaktree's social media refers to Oaktree's official social media platforms, such as Oaktree's official Facebook Page and Instagram account. Only authorised Representatives may access Oaktree's social media. The authorised Representatives listing will be determined by the Digital Communications Director.

6. Prohibited use

Oaktree's IT must not be used in any way that may negatively impact the organisation's reputation, compromise personal productivity, offend other Representatives or adversely affect Oaktree's technology systems. Representatives are expressly prohibited from using Oaktree's IT for any activity that is illegal under any state or federal legislation.

Oaktree's IT is not to be used, without limitation, for the following:

a) accessing, distributing or storing material that may constitute harassment, sexual harassment, bullying or discrimination on any prohibited ground including race, sex, disability, religion or sexual preference (for more information see our Anti-Discrimination, Bullying and Harassment Policy),

b) accessing, distributing or storing material of a pornographic, offensive or otherwise inappropriate nature,

c) uploading, downloading or making available any material that contains viruses or any other computer code, files or programs designed to interrupt, destroy, or limit the functionality of any computer software, hardware or Oaktree's IT,

d) infringing a third party's intellectual property,

e) pretending to be anyone, or any entity that Representatives are not,

f) distributing defamatory, abusive, threatening or otherwise offensive messages,

g) distributing chain-mail or spam,

h) in any manner that may be unprofessional or offensive, or cause embarrassment or reputational risk to Oaktree, or

i) to access Oaktree information which Representatives are not authorised or entitled to view.

7. Cyber Security

Oaktree's IT Facilities contain information that is confidential and sensitive. Representatives are issued an individual account to access Oaktree's IT Facilities and should undertake the following steps to maintain the security of Oaktree's IT.

7.1 Passwords

Representatives should create a secure password for their Oaktree Facilities. The password should be kept confidential. It should not be disclosed to anyone external or from Oaktree, except the CFO and Director of Legal when specifically requested. Representatives must not attempt to access another Representative's email, unless express permission is granted.

7.2 Use of Facilities

Facilities are to be treated as confidential and should only be shared with other Representatives who require access. Representatives must only use IT Facilities in ways that are relevant to their role. Representatives are required to delete documents in accordance with Oaktree's Privacy Policy.

To assist with personal security, any Representative that is logged into a system should lock the screen of that system when they are not present at their machine.

7.3 Accessing Facilities

Oaktree Representatives should consider the security risks involved when accessing Oaktree's online Facilities. Secure Wi-Fi routers should be used when engaging in such online Facilities as the use of open public Wi-Fi routers pose a high cyber security risk. Representatives should endeavour to use their own private devices when accessing Oaktree Facilities, and avoid using public computers that pose a high cyber security risk.

7.4 Oaktree's information

Information belonging to Oaktree should only be shared with approved parties and sent via secure channels such as through Oaktree email accounts, Google Drive or Dropbox. If a Representative is in possession of any of Oaktree's information without approval, they must return or destroy all such information at the election of the person who owns that information. Oaktree may take disciplinary action against them.

Information belonging to Oaktree should only be printed where needed, especially confidential information. When printed, it should be safely stored with access limited to only those who require it. This must be done in accordance with Oaktree's Privacy Policy.

7.5 Information Back-up

Information loss is a key cyber risk for Oaktree. Team managers are responsible for backing-up their team's documents. A full document back-up should be done every two months on the platform Multcloud. This could include a backup of the team's Google Drive folder and Dropbox documents. Representatives should ensure that documents are stored on these platforms and not their personal devices.

7.6 Social Media and NationBuilder

The information stored on Oaktree's social media sites and NationBuilder database is valuable to Oaktree's operations. As such, a limited number of Representatives should have the ability to edit these sites. Where possible, strategies should be put in place to limit the ability of any one Representative to tamper with the social media sites.

7.7 Suspicions

Representatives that receive suspicious emails should first verify the email with the sender before opening the email and downloading or clicking links within that email. Representatives should not access suspicious websites, any websites that they do not trust or engage with any suspicious activity while using Oaktree's Facilities. Should any Representative engage in suspicious online activity, they should report this to the Chief Financial Officer at cfo@oaktree.org immediately. They will be expected to fully cooperate in Oaktree's investigation and rectification of any such activity.

8. Termination of employment or relationship

Upon termination of their relationship with Oaktree, Representatives must:

a) return all Oaktree information and Oaktree IT Facilities to Oaktree,

b) clear all saved passwords on their personal devices that provide access to Oaktree IT, and

c) If they still have access to Oaktree IT, ensure that they are not still holding themselves out as being a Representative of Oaktree.

This clause continues to apply after Representatives leave Oaktree.

9. Breach of policy

Failure of Representatives to comply with the standards set out in this Policy may result in disciplinary action including termination of their employment or engagement with Oaktree.

It is each Representative's obligation to ensure that they understand how this Policy applies to them. If a Representative is uncertain about whether this Policy applies to them, or a particular situation, or has any other questions, they should speak with their manager or contact the legal team at legal@oaktree.org or complete the form on www.oaktree.org/you.

Annexure 1

Nation Builder Access

Access to Nation Builder will operate in the below manner:

1. Chief of Staff is in charge or removing and granting access to Nation Builder such access will only be granted to those who require it.

2. Head of Marketing and Fundraising oversees the management of Nation Builder. This includes;

   - how it is used,

- who requires access,
- what level of access they require, when giving people high levels of access it is important that we have a clear reason for why they require this access,