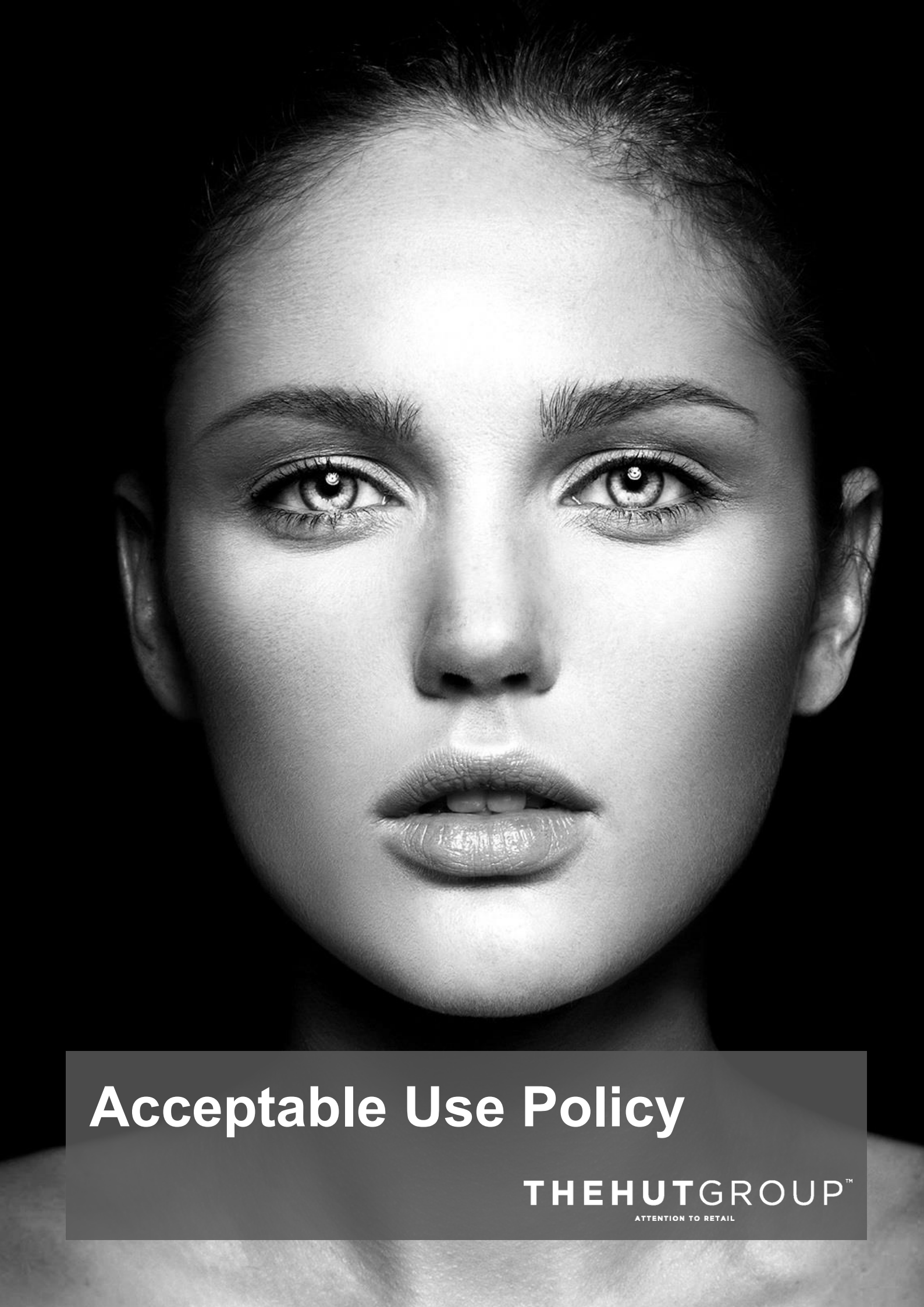

Acceptable Use Policy

THEHUTGROUP™

ATTENTION TO RETAIL

Version: v1.0
Effective: March 2016
Owner: Graham Thomson, Chief Information Security Officer

Version History:

Version	Author	Description	Reason for Amendment	Date	Next review
1.0	Peter Stanfield	Live	Creation of THG Policy	10/03/2016	01/01/2017

Contents

1. Introduction

The Hut Group has a responsibility to ensure that its technology systems are used in a reasonable, responsible and legal manner.

This document details the mandatory requirements that The Hut Group has set for using its technology systems. It applies to all The Hut Group business units, operations, functions, and staff, including permanent and temporary employees and third-party personnel such as agents, temporaries, contractors, and consultants, who have access to The Hut Group's technology systems, herein referred to as Staff.

All use of The Hut Group technology systems must be reasonable and appropriate. By using The Hut Group's technology systems, Staff accept and agree to abide by the terms of this policy.

Any employee found to have violated the requirements of this policy, either by negligence or by intent, may be subject to disciplinary action, up to and including termination of employment.

2. What technology systems are covered by acceptable use?

All technology systems owned, leased and/or managed by The Hut Group are in scope for Acceptable Use. These include, but are not limited to The Hut Group's:

- company internet services (e.g. internet access from the office and company WiFi services)
- company email and other communication systems used for THG business
- phones used for THG business
- company computers (e.g. laptops, desktops, macs, tablets, servers, etc)
- company facsimile, post and courier services

3. What is acceptable use?

Acceptable Use simply refers to use of our technology systems that is legal, reasonable and appropriate for your job role.

Specific examples of what is considered to be 'unacceptable use' are detailed below (this list is not exhaustive but is intended to indicate by example what constitutes a breach of this policy):

- use that negatively infringes The Hut Group's brand and reputation
- theft or unauthorised disclosure of The Hut Group's INTERNAL or CONFIDENTIAL information (e.g. personal data, customer records, staff records, payment card information, confidential business plans, etc)
- copyright or intellectual property rights infringement
- sharing of passwords and authentication credentials for The Hut Group's technology systems (note: Staff are personally responsible for all actions that take place with their credentials)
- creating, circulating or intentionally accessing any material which contains extremist, subversive or terrorist material
- creating, circulating or intentionally accessing images which contain nudity or scenes which could cause offence to other staff
- intentional or careless transmission of computer viruses and other malicious code (malware)
- any use that could breach the security or availability of The Hut Group's technology systems
- accessing or attempting to access The Hut Group's information or systems that the user is not authorised to access, including attempts to elevate access rights
- computer hacking, internally or externally, and intentional disruption of the network
- excessive personal use of The Hut Group's technology systems
- use of unauthorised internet proxy sites or any attempt to anonymise or hide internet use
- running a personal business, including unauthorised selling/advertising of goods or services
- transmission of defamatory, hurtful or harmful material including use of language that could be judged by The Hut Group as sexual, religious or racial harassment
- behaviour considered to be bullying or harassment
- inappropriate gambling
- any activities of an illegal or unlawful nature

Staff must store and process all The Hut Group's information (whether classified as PUBLIC, INTERNAL, or CONFIDENTIAL) in line with the requirements detailed in the Information Classification and Protection standard. This includes keeping a 'clear desk' by ensuring that confidential information, laptops and mobile phones are secured when unattended.

To protect our business and our staff from internet based threats, The Hut Group reserves the right to block access to certain categories of website that it considers inappropriate. If access to a blocked site is required for legitimate business purposes, then the user must contact the Service Desk to request access. Access must then be authorised by your line manager.

4. What are the risks of unacceptable use?

Unacceptable use (i.e. illegal, damaging or inappropriate actions by Staff, whether knowingly or unknowingly) could result in:

- financial losses and fines
- reputational damage from adverse publicity
- damage to customer relations
- loss of system availability leading to a reduction in productivity
- legal action or
- criminal investigations

Staff should keep in mind that The Hut Group can be held responsible for the content of emails sent and that they can be reproduced in a court of law in the same way as written statements.

Staff must report known or suspected breaches of this policy to their line manager or the Information Security team.

5. Privacy and monitoring

The Hut Group retains the right to log and/or monitor its technology systems in line with local law and regulations for the purposes outlined below. Staff should not have any expectation of absolute privacy in all circumstances as to their use of The Hut Group's technology systems, subject to local law.

The Hut Group will log, monitor and/or analyse communications for the following purposes:

- record keeping
- ensuring compliance with regulations and laws
- preventing and detecting criminal activity
- investigating or detecting inappropriate use
- checking for viruses and other malicious code (malware)
- ensuring business continuity (e.g. accessing critical communications when Staff are absent from work due to holiday or sickness)
- investigating a breach of any The Hut Group policy, standard or employment terms
- monitoring standards of service, staff performance and for staff training
- grievance, disciplinary or legal investigations

Incoming faxes, post and packages will be treated as business correspondence and may be subject to security screening which could include an examination of the contents. You should be aware that all such correspondence may be opened in your absence from the office.

The Hut Group's communications may be disclosed to third parties without notice to Staff for the purposes of investigating possible violations of this and other The Hut Group policies, routine maintenance, preparing for or responding to any legal or regulatory actions, claims or processes and as The Hut Group deems necessary.

Staff need to be aware that monitoring processes might reveal sensitive personal data about them. By using The Hut Group's technology systems for personal activities Staff consent to The Hut Group processing any personal data which may be revealed by such monitoring.

6. What is acceptable personal use?

The Hut Group's technology systems are the Company's property and are made available to Staff for business purposes. However, Staff may use The Hut Group technology systems for brief and reasonable personal use.

Staff must ensure that their personal use does not interfere with the performance of their duties or take priority over work responsibilities. If there is uncertainty about what is considered reasonable personal use, Staff should consult their line manager.

All personal mail which is placed in the post tray for external delivery must be stamped with sufficient postage. Personal mail must not be franked at the company's expense.

Personal use may be restricted or withdrawn if any use is deemed unacceptable.

The Hut Group does not accept responsibility for any loss, costs, claims or damages suffered by any user when using its technology systems for personal use.

7. Telephone acceptable use

Company employees may receive or make personal calls during break periods only. For reasons of security, privacy and a courtesy to other staff members it is prohibited to take these kinds of call in the office work areas.

Telephones provided at work stations are to be used to conduct company business ONLY (this is without exception).

8. Remote working & remote access

Remote working is defined as "working with THG information when outside of company buildings" (e.g. working on your company laptop or paper documents from home, 3rd party offices or hotels).

Remote access is defined as "accessing The Hut Group's internal network from a computer outside company buildings" (e.g. from your home, external wifi hotspots, 3G connections and 3rd party offices). Note that this excludes email synchronisation on personal or company phones. The official remote access solution is required to be able to have remote access to the internal network.

The requirements of this policy also apply when working remotely.

Remote access from non THG computers

- The Hut Group's information must NOT be stored on personal computers (i.e. when using the remote access solution do not copy files to your personal computer).
- The Hut Group's information must not be stored on any web-based storage service unless it is expressly approved by the Service Desk for business purposes. Examples include but are not limited to: iCloud, Dropbox, Google Drive, One Drive, and personal email accounts.
- If you require offline, out of office storage of THG information please request a company laptop.
- You must have up to date anti-virus (aka anti-malware) software installed on non THG computers used for remote access. If you do not have an anti-virus product, free software is available, including:
    - For PCs and Macs: https://www.sophos.com/en-us/lp/sophos-home.aspx

Physical access control

- You must ensure that no one else can access The Hut Group's network during your remote access session.
- Do not leave your computer unattended while the session is open (use screen lock, or log off). Log off when your work has finished.
- Physically secure company laptops and paper documents when not in use in public places (i.e. lock it in a hotel safe if left in a hotel room, or lock it in the boot of your car if left there).

Lost or stolen assets

- You must report lost or stolen remote access tokens, THG laptops and mobiles, USB storage with confidential files, and confidential paper documents to the Service Desk as soon as possible.

9. Social media

Social media includes any website in which visitors are able to publish content to a larger group. Examples include but are not limited to: Facebook, Twitter, YouTube, Google+, Wikipedia, Instagram, Vine, Tumblr, LinkedIn, blogs, Reddit.

Staff may only post material on social media platforms in The Hut Group's name (whether using our name or on our behalf) if they have been specifically authorised to do so by their manager, and that the content has also been approved by the business.

Posting of content to corporate sponsored social media (e.g. the MyProtein Facebook page) is permitted only for members of the Social Media & Customer Relations team to publicly represent any of The Hut Group's brands.

Personal use of social media is not permitted during usual work hours, with the exception of occasional personal use during break times, subject to any such use not interfering with business activities and such use complying with the rules set out in this policy. Permission to use social media in this way may be withdrawn by us at any time, at our discretion, and without notice.

Employees, affiliates and/or ambassadors of any THG brands shall not mention direct competitors in the course of any of their publically available communications in a way that could be construed as negative in nature without prior written approval by the Legal division of THG. Failure to adhere to this requirement could result in disciplinary action being taken.

When you are using social media please take in to consideration the below factors:

You must:

a) make it clear in any social media postings, or in your personal profile, that you are speaking on your own behalf and any views expressed are yours;
b) be respectful to others when making any statement on social media and be aware that you are personally responsible for all communications which are published on the internet for anyone to see;
c) ensure that your profile and any content that you post are consistent with the professional image you present to clients and colleagues;
d) report to your line manager any social media content that breaches any of the above rules and/or which disparages or reflects poorly on us; and
e) seek and obtain advice from your manager or a member of the Human Resource team before making a post on social media, if you are unsure if such post will be in breach of the above rules.

You must not:

a) make any social media communications that could damage our business interests or reputation, even indirectly;
b) use social media to defame or disparage us, or our staff or any third party; to harass, bully or unlawfully discriminate against staff or third parties; to make false or misleading statements; or to impersonate colleagues or third parties;
c) post offensive or pornographic material;
d) post comments about sensitive business-related topics, such as our performance, or do anything to jeopardise our trade secrets, confidential information and intellectual property. You must not include our logos or other trademarks in any social media posting or in your profile on any social media;
e) post any information relating to our staff, customers, competitors, suppliers and any of our other stakeholders;
f) post anything that may render us liable, whether for prosecution or to a third party; and
g) use any email address given to you by us, or which we have permitted you to use for the purposes of carrying out your duties, to register with or use social media platforms.

The Hut Group reserve the right to monitor and review, without further notice, social media platforms for legitimate business purposes and/or where we suspect that these rules may have been (or likely to be) breached.

The Hut Group may require a member of staff to remove any social media content that it considers to constitute a breach of this policy. Failure to comply with such a request may results in disciplinary action in itself.

It is also your responsibility to report any instances where you discover colleagues, affiliates or ambassadors of The Hut Group operating outside of the above terms. Please ensure you advise them to cease or report this by emailing compliance@thehutgroup.com.

A breach of any of the above rules relating to social media use may be considered to be gross misconduct which could result in your summary dismissal.

10. Breaches of the policy

A breach of this Policy is defined as:

- Any non-compliance with this Policy where there is no approved exception; or
- Failure or inadequacy of any minimum security control that has been implemented, whether or not it has resulted in an incident.

Non-compliance with this Policy (where there is no approved exception) may be treated as a disciplinary matter.

All breaches must be reported to the Information Security team in a timely manner.

11. Where can I find further help and information?

This Standard is owned by the Chief Information Security Officer and all questions or queries regarding it should be directed to:

- Information.security@thehutgroup.com