HUNTSWOOD

ACCEPTABLE USAGE POLICY ASSOCIATE VERSION

APPROVAL CONTROL

ROLE	NAME	DATE
Chief Technology and Risk Officer	Steve Mills	09/04/2018
Chief of Staff	Sara Robinson	10/04/2018
Risk Director	Helen Maslin	28/04/2021

VERSION CONTROL

VERSION	AUTHOR NAME	VERSION CHANGES	DATE
4.0	Ethan Moore	Sign off complete	10/04/2018
4.1	Beth Eckles	Minor amendments to spelling	19/04/2018
4.2	Carol Hawker	Review	23/03/2019
4.3	Carol Hawker	Review – Removed reference to Skype and replaced with Microsoft Teams	23/03/2020
4.4	Carol Hawker	Annual Review and sign off by Risk Director – Minor amends	28/04/2021
4.5	Craig Wooster	Annual review. Change of owner title	12/01/2022

TABLE OF CONTENTS

OBJECTIVE

Huntswood's Acceptable Usage Policy gives clarity on the acceptable use of information and of assets associated with information.

Where any reader feels this policy is unclear or becomes aware of any potential or perceived risk to the information security of Huntswood, its Clients or their Customers then they have the general obligation to act responsibly to protect information and raise their concerns with the Information Security Manager.

APPLICABILITY

This policy applies to all Huntswood Group representatives. It is every Huntswood representative's responsibility to ensure that they read, understand, and adhere to the Acceptable Usage Policy.

POLICY PRINCIPLES

1. Authorised System User

As a Huntswood representative you can consider yourself as an authorised user for a specific piece of information, software, hardware, or computing facility (asset) only if you have been given a unique user ID to access it from Technology.

User IDs are given to individuals for their own use only. Allowing others to use your unique user ID is not acceptable.

Attempting to access Huntswood computing facilities when you are not an authorised user is considered gross misconduct.

Unauthorised access to an information system is also a breach of the Computer Misuse Act 1990 and if found guilty could lead to a fine, imprisonment or both.

2. Passwords

Passwords are utilised to authenticate the identity of the individual using the user ID. They are for the individuals use only. Therefore, allowing others to use your password is not acceptable.

a. Account/Email Passwords

Account and Email passwords must be at least 10 characters in length and contain at least 3 of the following character types:

CHARACTER TYPE	EXAMPLE
English Uppercase Alphabet Characters	A-Z
English Lowercase Alphabet Characters	a-z
Base 10 digit	0-9
Non-Alphanumeric Characters (Special Characters)	!$#,%

b. Mobile Device Passwords

Mobile Device passwords, e.g. iPhones or iPads must be at least 6 characters in length and contain at least 3 of the following character types:

CHARACTER TYPE	EXAMPLE
English Uppercase Alphabet Characters	A-Z
English Lowercase Alphabet Characters	a-z
Base 10 digit	0-9
Non-Alphanumeric Characters (Special Characters)	!$#,%

The use of the word ‘password’ or its derivatives is not acceptable.

Passwords must not:

- Contain the user ID or parts of the user’s full name
- Be easily guessed or identifiable to the user i.e. Huntswood, favourite football team, partner’s name, pet’s name, date of birth, post code, season or year i.e. ‘Winter2018’.
- Be a word in the dictionary

If a password has been divulged to someone else or it is believed that a password has been used or is known by someone else, then it must be changed immediately.

All passwords should be unique, it is not acceptable to use the same password across multiple logins and devices such as your laptop and mobile phone.

It is not acceptable to write a password down or store it in an office document; for example, Word and Excel (unless this is password protected).

Any equipment that contains default passwords must be changed before being used and especially before being attached to Huntswood's network and computing facilities.

3. Access Control – Access Cards/ID Passes

Access cards/ID passes are given to allow access into offices that you need access to. The Access Control Policy sets out the company position on the issue of cards and control measures in place.

Access cards for Huntswood buildings remain the property of Huntswood and it is the responsibility of the card owner to keep the card secure at all times.

Attempting to access a secure area that you do not need access to, is not acceptable and nor is allowing another person to use your access card.

Allowing members of the public or unknown visitors through any access-controlled barrier, door or into any secure area by the use of your access card (tail gating) is not acceptable.

If an access card is lost or stolen Reception must be informed immediately to cancel the card and reduce the risk of an information security event from happening.

4. Access Control - Visitors

As set out in the Access Control Policy, all visitors to Huntswood must be met by a host, who is responsible for ensuring that their visitors sign in and out and each receive a visitor's badge, which are obtained from reception.

Visitors must always wear their visitor badges in a prominent position when within Huntswood offices.

If a visitor is not wearing a visitor badge or there is a suspicion about their identity or purpose, you are encouraged to ask the visitor who they are meeting with and whether they have collected a visitor badge.

If you feel uncomfortable doing this then speak with a manager who can deal with the situation.

Any visitor without a visitor badge must be escorted back to reception and the host informed.

It is important that you do not put yourself or anyone else at risk by questioning a visitor. If you are working alone or feel threatened, alert a colleague, or dial 999 and ask for the Police.

The host is responsible for ensuring that their visitors know and understand the emergency evacuation procedures. Visitors must be fully aware of their nearest fire escape.

If a visitor breaches Huntswood's Information Security Policy, then an information security incident must be logged as soon as possible. Please follow the incident management policy, which can be found on the 'the Group document repository' or contact iso@huntswood.com.

5. Information Classification

Information covered by the Classification and Labelling Policy must be dealt with as instructed in that policy at all times.

a. Clear Desk

Huntswood operates a clear desk policy, which means that only information required to do the job in hand should be kept in view. This is to reduce the risk of unauthorised access to information.

When left unattended, desks must be clear and tidy at all times.

Most printers work on a 'follow me' basis, however where these are not in place, information sent to a printer must be collected immediately. Should unattended printing be found on a printer this must be disposed of in the confidential shredding bin provided.

Paper based information classified Private or above must be disposed of in the confidential shredding bin provided and not be placed in any of the general waste or recycling bins.

If the confidential shredding bin is full, do not place the waste on top or around the bin or leave it hanging out of the letter box slot. Use another confidential shredding bin and inform Reception.

Always consider the classification/sensitivity of information on your desk as others around you may not be authorised to view the information.

b. Clear Screen

When left unattended, computer screens must be locked. This is to prevent the risk of unauthorised access to information.

Always consider the classification/sensitivity of information on your screen as others around you may not be authorised to view the information.

Microsoft Windows PCs are locked by pressing the <WINDOWS> + <L> keys or <CTRL> + <ALT> + <DELETE> keys and then selecting 'Lock this computer' from the menu that appears.

Apple Mac computers are locked by selecting the Apple icon and then selecting 'Sleep' from the menu that appears.

If you see a computer unattended and not locked, then lock the computer immediately. Do not use the computer for any reason as this is unauthorised access (we are all responsible for Huntswood's security).

People who routinely work with sensitive data, e.g. HR, Legal or Finance should consider the use of a privacy screen to provide additional security.

6. Protection against Malicious Code – Virus Protection

To protect against malicious code (any software that does damage to the computer that it runs on or doesn't do what the user expects it to do), Huntswood deploys protection hardware and software.

To protect from malicious code, Huntswood installs “Trend Micro OfficeScan”, which is always running.

If you discover that OfficeScan is not running either because the icon is not present or does not have the green tick, do not use the computer, and report it to the Technology Service Desk (this can be checked by looking in the “System Tray” by the clock and making sure the following icon appears
 .

Using a computer without OfficeScan running or attempting to disable, remove or circumvent OfficeScan on it is not acceptable.

If you receive an email or message stating that you are infected with a virus, do not act upon the contents of the email or message, report it immediately to Technology Service Desk for investigation.

7. Removable Media

Removable media can be defined as any device that can store information that can be removed from Huntswood’s computing facilities and premises.

Examples of removable media are, but are not limited to: USB memory drives, memory sticks, flash drives, flash cards and digital cameras.

Do not connect or attempt to connect any unauthorised USB devices or peripherals to your computer. If you are unsure if a device or item is authorised or if it is genuine seek guidance from your manager, the IT Service Desk, a member of Technology or the iso@huntswood.com.

Use of removeable media is limited to ‘read-only’. If access to add information to removeable media is required, then the user must contact the Technology Service Desk.

8. Mobile Devices

A mobile device can be defined as any device that is designed to be used outside of the normal office environment. Examples of mobile devices include, but are not limited to: Laptops, mobile phones, smart phones, PDAs and tablet devices.

Mobile devices are provided to individuals in specific roles primarily for business use, but it is accepted that you may from time to time use your Company mobile phone for personal calls and this usage should be reasonable. Please do not use your Company mobile telephone to text or call premium numbers. Use of your company mobile telephone may be monitored to prevent abuse of the facility.

To prevent theft and breaches of confidentiality, leaving a mobile device unattended in a public place is unacceptable. When not in use, mobile devices must be locked so that a password is required to access it in line with section 2 (Passwords) of this policy. Mobile devices must be kept in a secure environment when unattended.

A secure environment is considered to be:

- Huntswood’s offices; Locked either in a drawer, cabinet or storage locker with the key removed.

- At home; Ensure the mobile device cannot be seen from a window. It is expected that basic security is followed to prevent a break in i.e. locking doors and windows and they are of good and sound construction.
- Hotel room; when unattended, mobile devices must be stored in the safety deposit box.

Locking your mobile device in the boot of your car when parked is not a secure environment and wherever possible this must be avoided.

UK law states it is illegal to text or make a phone call (other than in an emergency) using a hand-held mobile device, it is also illegal to use mobile phones to take photos or videos, scroll through playlists or play games while driving. Drivers can use a mobile device 'hands-free' [using a Bluetooth headset, voice command, in-car system) while driving, for example sat-nav, if it's secured in a cradle or appropriate fixing. We would strongly advise not to make phone calls whilst driving and that you switch your phones to voicemail. Huntswood will not reimburse or compensate any individuals for any fines or points that they may incur.

If you need to use your mobile device when driving, park up, switch off the engine and remove the keys.

Eavesdropping is used by identity thieves and for corporate sabotage. Care must be taken to not divulge confidential or company/client sensitive information when talking or video conferencing on mobile phones or devices in a public place. Where possible, rather than discussing confidential information in a public place send an email.

Care must also be taken when using a mobile device in a public place. Check who is behind you and make sure that they can't see your screen. Additionally, you should not connect to a public Wi-Fi connection as these are not guaranteed to be secure.

Make sure that if you are reading paper-based information no one can read the document as you are reading it.

When not in a secure environment, it is not acceptable to discuss, read or have on your mobile device's screen, information classified Restricted or above. Please see Huntswood's Classification and Labelling Policy, which can be found on the 'group document repository'.

When outside of Huntswood offices, laptop users are required to use a VPN to connect to the Huntswood network. Attempting to connect to the Huntswood corporate network using a computer without the approved VPN software it is not acceptable. Attempting to disable, remove or circumvent the VPN software on a Huntswood device is not acceptable.

9. Lost or Stolen Mobile Devices

If your mobile device is lost or stolen, you must inform your line manager immediately.

As soon as possible, log an information security incident. Please follow the Incident Management Policy, which can be found on the 'group document repository' or contact the Information Security Manager at iso@huntswood.com

10. Use of Software

Software is usually protected by copyright. Using software which you are not entitled to use is a breach of the Copyright, Design and Patents Act 1988. A serious breach of copyright is a criminal offence and if found guilty, could lead to a fine, imprisonment or both. The

Technology department is responsible for controlling software in line with policies and procedures approved by the Chief Technology Officer.

Only software approved by the Technology department can be purchased, installed, and used on any of Huntswood's computing facilities. Attempting to install or use personal software without approval is not acceptable.

11. Inappropriate Material

Huntswood has a legal obligation to protect its employees from material that may cause offence or distress (Obscene Publications Act 1959) and we expect everyone to be respectful to their colleagues, clients and the public at all times.

Inappropriate material is considered any material that is likely to cause offence or distress to another person or persons.

It is not acceptable for anyone to attempt to gain access to, store or distribute inappropriate material using Huntswood computing facilities. If you are unsure, please speak to your line manager.

The following is a non-exhaustive list of examples of material that are considered inappropriate:

INAPPROPRIATE MATERIAL
Abusive
Bad taste
Defamatory
Derogatory against someone's age
Derogatory against someone's disability
Fetish
Homophobic
Political and religious extremes
Pornographic
Racist
Sexist

12. Internet Usage

Standard internet services are provided primarily for business use, but it is accepted that you may from time to time use the internet for personal use and this usage should be reasonable.

Internet usage is monitored to prevent abuse of this facility and to support Huntswood's security policy, prevent breaches of UK and EU law, to protect against data leakage and to prevent Huntswood from falling into disrepute. Just because you can access a website, doesn't mean that you should. Downloading copyright protected material is not acceptable unless

written agreement from the copyright owner is received in advance and passed to Huntswood's Legal Team. The use of the following sites, but not limited to, is not acceptable:

- Those containing inappropriate material.
- Those that are illegal in the UK.
- Those that breach copyright, this includes peer-to-peer (P2P) file sharing sites

Due to the high risk of malware and to protect against data leakage, the use of personal webmail facilities is not acceptable, for example, Gmail, Hotmail, Apple and Yahoo. Personal Instant Messaging services (IM) is also not acceptable, for example, WhatsApp. Work or business related instant messaging is only permitted using Huntswood authorised messaging tools such as Rocket Chat, TEAMS for Business or the instant message function in Yammer on company provided workstations/laptops or mobile devices.

Attempting to or using sites designed to bypass Huntswood security controls will be seen as gross misconduct, for example, proxy avoidance sites.

Approval for use of non-business websites for personal use are to be approved by the People Director or Chief Risk Officer.

Computing facilities used for Client and Customer data processing will be barred from general internet access and only sites approved for the Client project will be allowed.

13. Email

Email is provided primarily for business use, but it is accepted that you may from time to time use Email for personal use and this usage should be reasonable. Huntswood's Email Policy, which can be found on the 'group document repository', provides further details on the use and monitoring of emails and what is acceptable.

Sending Huntswood or client related information via email, or any other means, to your personal email address from your Huntswood mailbox or using your personal email address to send emails on behalf of Huntswood is unacceptable.

Messages, external or internal must only be sent to person for whom they are intended. The style and content of an e-mail message must be consistent with Huntswood's standards and house style for all written communications. Information of how to set this up can be obtained from the Marketing team.

Sending email containing inappropriate material such as, but not limited to, abusive, racist, discriminatory, or defamatory is unacceptable as is sending trivial messages, forwarding of humorous stories or jokes and chain mail. If you are unsure, please do speak to your line manager.

14. Microsoft Teams

Teams is provided for business usage which should be kept reasonable and acceptable.

Communications using Microsoft Teams, whether external or internal must only be sent to the person(s) for whom they are intended. The style and content of a communication using Microsoft Teams must be consistent with Huntswood's standards for direct or written communications.

Sending communications using Microsoft Teams containing inappropriate material such as, but not limited to, abusive, racist, discriminatory, or defamatory is unacceptable.

Instant messages sent using Microsoft teams are recorded and stored within the Office365 environment. No client data should be transmitted using Microsoft Teams.

15. Information Security Incidents

All Information Security incidents are to be reported to the Information Security Manager (iso@huntswood.com). Please follow Huntswood's Incident Management Policy.

When you spot a potential information security weakness, it is very important that you do not attempt to prove it and thus cause an information security event.

16. Training

Information security training takes place regularly through workshops and exercises. New starters are inducted into the business and information security training is part of this induction process for all Huntswood representatives.

HR maintains a record of training as evidence of our commitment to information security and our people in giving them the relevant support needed to protect our information assets.

Engagement Managers are responsible for ensuring on-going training and compliance monitoring with any Client contractual or cultural alignment requirements.

17. Audit

As part of Huntswood's commitment to ISO27001:2013 (Information Security), annual audits will be undertaken by the Internal Audit function. These audits will include reviews of all controls within this policy and reports on findings and recommendations will be issued to The Board and Risk & Audit Committee as appropriate.

TABLE OF DEFINITIONS

The table of definitions provides definitions of terms used within the policy document

TERM	DEFINITION
Huntswood Representative	Permanent, temporary and fixed term employees, consultants, contractors, agents and subsidiaries acting for, or on behalf of Huntswood

POLICY RESPONSIBILITIES

The following table defines the business roles and their responsibilities in regard of the policy document.

RESPONSIBILITY	ROLE	DEFINITION
Owner	Chief Risk Officer	The Owner ensures the policy is reviewed and maintained on a regular basis
Reviewer	People Director	The Reviewer ensures the policy document aligns with relevant legislation and company requirements
Author	Risk & Audit Manager	Shall update the policy document in a succinct time frame on receiving updates from the reviewer and in accordance with company policy writing guidelines
Policy Audience	Huntswood Group representatives	Must apply the business policy to the business they undertake on behalf of Huntswood. A copy of the AUP must be read, agreed and signed before using any of Huntswood's computing facilities and before being assigned any Huntswood asset

APPLICABLE STANDARDS AND LEGISLATION

ISO27001:2013

Computer Misuse Act 1990

REFERENCE MATERIALS

Huntswood Acceptable Usage Policy and supporting policies and information is available to all Huntswood representatives via a link on the Timesheet Portal