REMOTE WORKING POLICY
CLIENT DELIVERY RESOURCE

APPROVAL CONTROL

ROLE	NAME	DATE
Risk Director	Steve Mills	26/05/2020

VERSION CONTROL

VERSION	AUTHOR NAME	VERSION CHANGES	DATE
0.1	Lucy Gilly	First Draft	31/03/2020
0.2	Lucy Gilly	Amends following review with Head of Risk and Risk Director	02/04/2020
0.3	Lucy Gilly	Amends following review with Head of Infrastructure and Senior Delivery Manager	07/04/2020
0.4	Lucy Gilly	Approved by Head of Operations	16/04/2020
0.5	Lucy Gilly	Approved for final version by Leadership Team	16/04/2020
0.6	Lucy Gilly	Minor drafting edits	22/05/2020
1.0	Steve Mills	Signed off	26/05/2020
1.1	Noel Hedges	Amends to include Return of IT Equipment	05/08/2020
1.2	Lucy Gilly	Approved by Legal and Commercial Director	05/08/2020

TABLE OF CONTENTS

INTRODUCTION

For the purpose of this policy, the term homeworking applies to remote working whilst performing services on behalf of the Huntswood Group ("Huntswood") for their end clients ("Huntswood's Client").

Huntswood will ensure that all users who work from home or remotely are aware of the acceptable use of portable computer devices whether those devices are provided by Huntswood, Huntswood's Client or owned by the individual providing the services. Should those portable computing devices be owned by the individual, then the acceptable use principles apply in the same manner.

Where portable computing devices are provided (or where those devices owned by the individual are used in provision of services to Huntswood's Client) to assist users to conduct official Huntswood business (on behalf of their clients) efficiently and effectively. This equipment and any information stored on it should be recognized as confidential sensitive valuable organisational information assets and safeguarded appropriately and in accordance with policy notified by Huntswood or Huntswood's Client from time to time.

Huntswood is committed to its duty to fulfil the requirements of the Equality Act 2010. Where reasonable adjustments are already made at an individual's display screen workstation, such as ergonomic and/or personalised equipment, that same help, support and protection shall be afforded to homeworkers. Should you require assistance in relation to this matter, please contact your team leader who will arrange for the appropriate action to be taken.

PURPOSE AND OBJECTIVES

The purpose of this policy is to establish the standards, working practices and supported configurations of remote working solutions during the provision of services to Huntswood's Client whilst working at home.

In response to the recent events surrounding the World Health Organisation ("WHO") classified pandemic for the COVID-19 'Corona' virus, Huntswood is taking steps to enable it to continue to provide services to its Clients.

Following unprecedented governmental guidance restricting travel, movement, large public gatherings and more general social interaction, companies from all sectors are experiencing severe business interruptions. The fast-paced evolution of the COVID-19 pandemic has brought with it new challenges for businesses almost daily.

In light of these circumstances, Huntswood and Huntswood's Client(s) have requested that we provision a working at home delivery of our existing services.

SCOPE

This policy applies to all temporary and contract personnel and representatives of Huntswood who are providing services to Huntswood's Client from home, or who have access to Huntswood Client's information, information systems or IT Equipment whilst working at home.

DEFINITION

This policy should be adhered to at all times whenever any user makes use of portable computing devices to process information of Huntswood's Client or access any system or software of Huntswood's Client regardless of the portable computing device used. This policy applies to all users' use of the Huntswood / Huntswood's Client IT equipment and personal IT equipment (collectively, "IT Equipment") when working on official Huntswood business away from the Huntswood or Huntswood's Client premises (i.e. working remotely).

IT Equipment and portable computing devices include, but are not restricted to, the following:

- Laptop computers
- Desktop Computers
- Tablet PCs
- PDAs
- Palm Pilots
- Mobile phones inc Smart phones
- Text pagers
- Wireless technologies

HEALTH AND SAFETY

For those individuals working at home remotely on a temporary basis as intended by the audience of this policy, then a formal health and safety assessment is not required. However, the individual is required to review and agree to the basic principles noted in Appendix B of this policy with any other requirements being notified to the appropriate line manager.

COMPUTER EQUIPMENT

There are several IT solutions to achieving a suitable working from home environment. The solution installed will largely depend on the type and quantity of work that the user will be undertaking at home and will largely be determined by Huntswood / Huntswood's Client processing requirements. This decision will be made in consultation between Huntswood IT and the IT department of Huntswood's Client.

Special attention will be paid to any requirement to use or access information that is deemed sensitive personal data.

In certain circumstances it may not be technically feasible to provide the IT facilities required for a user to carry out the services effectively from home. In these instances, your Team Manager must be informed immediately.

IT SUPPORT

If the individual uses their own IT Equipment, they will be responsible for any repairs or technical support related to that IT Equipment. Except where support is required in relation to software or applications installed on the IT Equipment by Huntswood's Client, in which case, Huntswood's Client shall provide technical support for the same.

Huntswood equipment will be repaired by Huntswood's IT department and Huntswood's Client shall be responsible for IT support for their IT Equipment.

RETURN OF EQUIPMENT

At the end of the engagement, the user is responsible for ensuring the safe return of the IT Equipment and any other equipment provided to the user in the provision of the Contractors Services by Huntswood or Huntswood's Client. The process for arranging the safe return of the IT Equipment will be communicated to the user at, or prior to, the end of the engagement by Huntswood or other such individual as notified to the user. The user is responsible for adhering to the requirements as communicated at that time. Unless otherwise agreed in writing, any cost incurred in returning the IT Equipment shall be borne by the user.

TELEPHONE

Where appropriate the Huntswood or Huntswood's Client will provide access to a telephony system. The user is not permitted to utilise their own telephone for the purposes of providing services, unless expressly authorised in writing by Huntswood and Huntswood's Client.

Any mobile telephone within the home environment cannot be used for the purposes of interacting with any information provided by Huntswood or Huntswood's Client in provision of the services. For the avoidance of doubt, a mobile telephone shall not be used to: record or store electronic notes, take or store pictures, record conversations for information related to the provision of services to Huntswood's Client or Huntswood.

OTHER EXPENSES

Expenses for heating, lighting etc., will not be reimbursed.

SECURITY

Huntswood's Information Security Policy must be complied with at all times. Huntswood's processing requirements as noted in Appendix A to this Policy apply to the processing of all Huntswood / Huntswood's Client information.

Huntswood's Client Information Security Policy must be complied with at all times, as should any written instruction from Huntswood's Client in relation to processing of Huntswood's Client information.

Users are responsible for the security of all data, howsoever held whilst providing services remotely. Written notes must not be taken relating to any information processed or accessed during the provision of services and printing should not be undertaken without prior written consent of Huntswood. Any paper must be stored securely to maintain confidentiality of information from members of the family or visitors.

Sensitive material or personal data must be disposed of by recognised methods using office based shredding equipment or other means. Further information on data protection is held within the Huntswood's Data Protection Policy and / or Huntswood's Client data protection policy as notified from time to time.

It is the user's responsibility to ensure that the following points are adhered to at all times:

- Users must take due care and attention of IT Equipment when moving between home and another site
- Due to the high incidence of car thefts laptops or other IT Equipment must **never** be left unattended in cars or taken into vulnerable areas.
- Users will not install or update any software onto a Huntswood / Huntswood Client owned portable computer device and where it is a user owned device, approval shall be sought from Huntswood / Huntswood's Client in the event the software interacts with any Huntswood / Huntswood / Huntswood's Client data
- Users will not install any screen savers onto a Huntswood / Huntswood Client owned portable computer device
- Users will connect with a secure network wired connection wherever possible. Where a wired connection is not possible and a wireless connection is used, this should be a secure connection. Sensitive personal data should **not** be accessed via public wireless connection.
- Users will not install any hardware to or inside any Huntswood / Huntswood Client owned IT Equipment, unless authorised by the Huntswood / Huntswood Client
- Users will allow the installation and maintenance of the Huntswood / Huntswood Client installed Anti-Virus updates immediately

- Users will inform the appropriate IT department of any Huntswood / Huntswood Client owned IT Equipment message relating to configuration changes

- No data relating to the provision of services to Huntswood or Huntswood's Client shall be stored on IT Equipment owned by the user and for those devices owned by Huntswood / Huntswood Client, data should be stored on a designated network drive and not held on the portable computer device

- All faults on Huntswood / Huntswood's Client IT Equipment must be reported to the appropriate IT department. Where a fault occurs on individual owned IT Equipment, where that fault may impact the processing of Huntswood / Huntswood's Client information, the individual must report that fault to their line manager.

- Users must not remove or deface any asset registration number

- User requests for upgrades of hardware or software must be approved by a team manager with appropriate authorisation. Equipment and software changes for personal equipment utilised in the provision of services to Huntswood / Huntswood Client shall be notified to Huntswood / Huntswood Client and if so required, Huntswood / Huntswood Client shall be provided access to the device to suitably configure and risk assess its suitability / security.

- No family members may use any IT equipment. The Huntswood / Huntswood Client provided IT Equipment is supplied for the user's sole use. Where a user utilises their own IT Equipment, the user should ensure that appropriate safeguards for securing access to the Huntswood / Huntswood Client environment are in place and approved by Huntswood / Huntswood's Client.

- The user must ensure that reasonable care is taken of the IT equipment supplied or used in relation to the services provided to Huntswood / Huntswood's Client

- The user cannot take any Huntswood / Huntswood's Client supplied equipment outside the United Kingdom. The IT Equipment may not be covered by the Huntswood / Huntswood's Client normal insurance against loss or theft and the equipment is liable to be confiscated by Airport Security personnel. Should you be using your own IT equipment, we would expect for you to notify your insurers of the intended travel and business use and ensure the IT equipment is insured for the duration of the provision of services to Huntswood / Huntswood Client. Further, we would expect you to notify Huntswood / Huntswood's Client of the intended travel.

- Huntswood / Huntswood Client may at any time, and without notice, request a software and hardware audit of any IT Equipment utilised in the provision of services to Huntswood / Huntswood's Client and may be required to remove any IT Equipment at the time of the audit for further inspection. All users must co-operate fully with any such audit

- Any user who undertakes work at home or remotely in relation to services provided to Huntswood / Huntswood's Client using their own IT Equipment must understand that they are not permitted to hold any database, or carry out any processing of information relating to Huntswood / Huntswood's Client, its employees or customers outside of the secure connection / segregated environment authorised by Huntswood / Huntswood's Client. **Under no circumstances** should personal, sensitive or secret information be emailed to a private email address or downloaded to the IT Equipment

- Any user accessing sensitive personal data, must only use Huntswood / Huntswood's Client IT Equipment unless written approval has been received from Huntswood's Client to agree the IT Equipment has appropriate technical security and advanced authentication mechanisms suitable for working remotely. Connection for this device must be with a wired connection and no wireless connections must be used.

- All IT Equipment owned by Huntswood / Huntswood's Client in provision of services shall not be used for any other purpose other than to provide the services to Huntswood / Huntswood's Client.

- All applications, software and installs required on any individual owned IT Equipment mandated by Huntswood / Huntswood's Client IT must not be removed, reverse engineered, tampered with or amended during the provision of services and any fault arising with those specific applications or software will require logging with the appropriate IT department.

- All Alexa and smart home devices must be turned off or removed from the working at home area to prevent any recordings.

Remote and Mobile working Arrangements

- Users should be aware of the physical security dangers and risk associated with working within any remote office or mobile working location.

- IT Equipment should not be left where it would attract the interests of the opportunist thief. In the home it should also be located out of sight of the casual visitor. For home working it is recommended that the office area of the house should be kept separate from the rest of the house. IT Equipment must be secured whenever it is not in use by either locking away in a cupboard or drawer.

- Users must ensure that access/authentication tokens and personal identification numbers are kept in a separate location to the IT Equipment at all times. Removable media devices are not permitted, and paper documentation must not be stored with the IT Equipment. Paper documents are vulnerable to theft if left accessible to unauthorised people. These should be securely locked away in suitable facilities (e.g. secure filing cabinets) when not in use. Wastepaper containing information related to the services must be shredded to required standards (DIN Level 4, Cross cut [1.9mm x 14mm])

Anti-Virus Protection

IT Equipment owned by Huntswood: Huntswood's IT department will deploy an up-to-date Anti-Virus signature file to all users who work away from Huntswood or Huntswood's Client premises whilst using a Huntswood device. Users who work remotely must ensure that their portable computer devices are connected to the Huntswood network at least once every two weeks to enable the Anti-Virus software to be updated.

IT Equipment owned by Huntswood's Client: Huntswood's Client will provide you with up-to-date information related to Anti-Virus requirements and any instruction related to the same must be followed.

IT Equipment owned by the user: must include Anti-Virus signature file suitable to the requirements of IT Equipment owned by Huntswood / Huntswood's Client and must be maintained for the duration of provision of services to Huntswood / Huntswood's Client.

Access Controls

It is essential that access to all information related to the services provided to Huntswood / Huntswood's Client is controlled and meets the requirements of Huntswood / Huntswood's Client. This can be done through physical controls, such as locking the home office and locking the computer's keyboard. In addition, this should be done logically by password or user login controls.

Portable computer devices should be switched off, logged off, or the keyboard locked when left unattended, even if only for a few minutes. All data on portable computer devices must, where possible, be encrypted. If this is not possible, then all Huntswood / Huntswood's Client data held on the portable device must be encrypted. A sufficiently secure remote access mechanism must be configured to allow remote users access to Huntswood / Huntswood's Client systems if connecting over Public Networks, such as the Internet.

Two separate means of authentication (i.e. username/password and Pin Safe PIN Number or Microsoft Two factor authentication app) must be used when accessing Huntswood / Huntswood's Client network and information systems (including Outlook Web Access / Office 365) remotely via both Huntswood / Huntswood's Client owned and non Huntswood / Huntswood's Client owned IT Equipment. Access to the Internet from Huntswood / Huntswood's Client owned IT Equipment should only be allowed via an onward connection (i.e. you must connect to the Huntswood / Huntswood's Client network first then access the Internet).

As compliance criteria on the Huntswood / Huntswood's Client becomes more complex the appropriate IT department may need to apply further security controls from time to time. Any such changes will be communicated to all users with remote access to Huntswood / Huntswood's Client software, systems. Such security controls may be applicable to Huntswood / Huntswood's Client owned and privately owned devices, should the user not wish their privately owned IT Equipment to be subject to security controls then that IT Equipment will not be allowed to connect to Huntswood / Huntswood's Client network or access Huntswood / Huntswood's Client information.

POLICY RESPONSIBILITIES

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

RESPONSIBILITY	ROLE	DEFINITION
Owner	Director of Risk	The Owner ensures the policy is reviewed and maintained on a regular basis
Reviewer	Head of Infrastructure	The Reviewer ensures the policy document aligns with relevant legislation and company requirements
Author	Head of Legal Services	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 Client Delivery Resource	Must apply the business policy to the business they undertake on behalf of Huntswood or Huntswood's Client

APPLICABLE STANDARDS AND LEGISLATION

A reference list of what standards, legislation and/or regulation the policy supports.

- ISO 27001:2013
- The General Data Protection Regulation (GDPR)
- Huntswood Client applicable legislation in accordance with notification from time to time

APPLICABLE POLICIES

- Information Security Policy
- Acceptable Use Policy
- Network Security Policy
- Data Protection Policy
- Applicable Policy of Huntswood's Client as notified from time to time

I hereby sign in acceptance and understanding of the policy principles required whilst working remotely.

Signature: **Name:**

Electronically Signed Date:

APPENDIX A

Processing Instructions

Definitions:

"Huntswood Information" means any information, including Personal Data relating to Huntswood or Huntswood's Client including, but not limited to; electronic, spoken and paper information accessed, used, created, maintained, disposed of, or otherwise handled in the course of user's performance of the services;

"EU Data Protection Laws" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

"GDPR" means EU General Data Protection Regulation 2016/679;

The terms **"Commissions"**, **"Controller"**, **"Data Subject"**, **"Member State"**, **"Personal Information"** **"Personal Data Breach"**, **"Processing"**, **"Supervisory Authority"** and **"Transfer"** shall have the same meaning as in the General Data Protection Regulation (GDPR), and their cognate terms shall be construed accordingly. Capitalised terms not otherwise defined herein shall have the meaning given to them in the Contract.

The word **"include"** shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

1.0 Data Processing

Any user shall:

1.1 process all Huntswood Information that it receives, is otherwise exposed to, is contained within systems or that is provided by Huntswood or Huntswood Client in accordance with;

1.1.1. the highest degree of confidentiality and to ensure that persons authorised to Process the Huntswood Information have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
1.1.2. in compliance with all applicable laws and regulations, including the EU Data Protection Laws;
1.1.3. the applicable Huntswood or Huntswood Client policies in force and as updated from time to time;
1.1.4. only in accordance with the reasonable instructions of Huntswood or Huntswood's Client, and to undertake measures reasonably requested by Huntswood or Huntswood's Client for data protection compliance, including,
1.1.5. the security requirements of the environment in which the services are performed.

1.2 only use such Huntswood Information for the purpose of fulfilling its duties under this Contract and shall not further disclose such Huntswood Information or transfer any of the Huntswood Information to any third party
1.3 not do (or permit anything to be done) which might cause Huntswood or Huntswood's Client to breach the EU Data Protection Laws in relation to the protection and transfer of Huntswood Information.
1.4 acknowledge and agree that nothing in the Contract is intended, nor shall it be construed, to permit the user to access, use, handle, maintain, process, copy, or dispose of any Huntswood Information for any purpose other than fulfilling its duties under the Contract.
1.5 acknowledge and agree that all Huntswood Information provided or made available by Huntswood or Huntswood's Client is and remains the property of Huntswood and/or Huntswood's Client
1.6 to ensure that appropriate technical and organisational measures are adopted to ensure safekeeping against unauthorised or unlawful Processing of Huntswood Information and against accidental loss, or destruction of or damage to the Huntswood Information, including taking all such measure as may be required to comply

with Article 32 of the GDPR and to notify Huntswood immediately if, in the user's opinion, an instruction from Huntswood or Huntswood's Client infringes EU Data Protection Laws.

1.7 in the event the instructions, physical and/or technical information security measures mentioned in clause 1.6 relating to Huntswood Information are not available, the user shall not process any Huntswood Information without first consulting with Huntswood or Huntswood's Client.

1.8 immediately upon becoming aware of a breach either by an individual user, and/or unauthorised or non-compliant loss or Processing of Huntswood Information that reasonably may have resulted in unauthorised access to Huntswood Information (including identification and detection of identity theft, pursuant the relevant industry best practice guidelines) individua user shall notify Huntswood and cooperate fully with Huntswood's investigation and response to the incident.

1.9 upon receipt of a request for information made pursuant to EU Data Protection Laws, the user shall, a) immediately notify the appropriate Data Protection Officer (as notified by Huntswood or Huntswood's Client from time to time) of the fact and content of the request, b) immediately consult with Huntswood regarding a response to the request; and, c) provide any information relating to the services, requested by Huntswood or Huntswood's Client.

1.10 except as otherwise required by law, not provide notice of any incident (as detailed in clause 1.8 or 1.9) directly to the persons whose information were involved without prior written permission from Huntswood or Huntswood's Client.

1.11 make available to Huntswood all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and, if requested, contribute to audits, including inspections, conducted by Huntswood or another auditor mandated by Huntswood, including without limitation any regulatory authority of Huntswood or Huntswood's Client.

1.12 upon termination or expiration of the services, the user will immediately return all Huntswood Information provided or made available from any IT Equipment, at Huntswood's election and in accordance with specifications for return or destruction that Huntswood or Huntswood Client shall provide at the time.

1.13 not use Huntswood Information supplied for targeted marketing purposes or any other prohibited purposes.

1.14 only make use of machines, systems, telephones and networking equipment that receive, process, interact with, transmit, or store Huntswood Information, that have been provided by Huntswood or Huntswood's Client, except where Huntswood or Huntswood's Client have expressly authorised and validated use of an individual's own IT Equipment.

1.15 not use any machine, system, telephone or networking equipment to receive, process, interact with, transmit, copy or store Huntswood Information not provided by Huntswood or Huntswood's Client. Any deviation must be approved in writing by the Huntswood or Huntswood's Client prior to use.

1.16 acknowledge and agree that Huntswood reserves the right to require the user to provide the results of a vulnerability scan, performed by a scanner approved by Huntswood of systems or equipment that are used in any way, or that interact with systems used in any way, to provide services and/or receive, use, process, maintain, transmit, store, or dispose of Huntswood Information.

1.17 acknowledge and agree that as a processor subject to the GDPR, disclosure of some or all of confidential information provided pursuant to the services, may be compelled pursuant to that law.

APPENDIX B

Health and Safety Guidance for Remote Working

WORKING IT EQUIPMENT REMOTELY:

- Raise your screen: Make sure your screen is raised so that the top of the screen is at eye level. This can be done using an adjustable laptop stand, a box or some books if necessary
- Use a separate keyboard and mouse - this enables the laptop screen to be positioned correctly
- Adjust your chair height if you can - your arms should be at right angles, with forearms lightly supported by the work surface. You may need a footrest if your feet are not firmly on the floor
- Make sure the lower back is well supported - support for your lower back will help encourage good posture. You can use a folded towel to give you more support or consider a back-support cushion if needed
- Take regular, short breaks: Move around for five or ten minutes every hour, aiming for frequent, short breaks
- Consider taking microbreaks to stretch, move around, change activity by taking a phone call, do some reading or get a drink to avoid prolonged static postures
- Take more frequent breaks if your DSE setup is not optimal or if you are experiencing discomfort

YOUR WORKING ENVIRONMENT:

- Be careful not to have any trip hazards such as trailing cables
- Make sure you have an adequate working temperature (Minimum 16 °C)
- Ensure that you have adequate lighting

TRY TO AVOID:

- using phones or tablets for a long time
- sitting on unsupportive seating such as a sofa
- static postures

Whilst it may seem easier to simply open the laptop and start working without making any adjustments, this can lead to poor posture, which can cause pain and discomfort over time.

It is well worth taking a couple of minutes to set up your workstation correctly each time you sit down to work. And remember, you can also stand up to work if that's more comfortable, for example on the kitchen worktop.

If you have any concerns about having somewhere suitable to work when you are at home please speak with your line manager and we will review how we can assist you.

The Health and Safety Executive (HSE) advice can be found here