RIDGE

ACCEPTABLE USE OF ASSETS POLICY

CONTENTS

1. DOCUMENT CONTROL

1.1. Distribution

This document, once issued, becomes a live document and, subject to updates and changes, shall be maintained as a configuration-controlled item. Any subsequent amendments must be submitted to the Systems Manager and controlled using document versioning.

DISTRIBUTION
All internal staff
Relevant external parties

1.2. Version Control

VERSION	DATE	DESCRIPTION	CREATED BY	REVIEWED BY
1.0	27.11.2021	Creation	LS	DW
1.1	24.01.2022	Review	LE	DW

1.3. Applicable Documents

DOCUMENT TITLE	DOCUMENT LOCATION

1.4. Definitions and Abbreviations

ACRONYM	DEFINITION
EEA	European Economic Area

2. INTRODUCTION

It is important that all staff members that are provided access to Ridge assets, systems and information are aware of their responsibilities.

This policy should act as a point of reference for all persons performing work for Ridge using ridge assets, systems or information. Further specific details on the operational elements of these assets or systems will not exist within this document and users should refer to Ridges' other policy and process documentation.

3. DATA CONTROL, LEGISLATION, AND INTELLECTUAL PROPERTY

3.1 Any information shared with Ridge or stored on a Ridge system that is not required for employment is done so at the employees own risk.

3.2 Persons performing work under Ridge should ensure that they abide by any legal and contractual requirements in respect to the use of computer use. This includes privacy and data protection regulations.

3.3 All work conducted for Ridge is Ridge's intellectual property, unless explicitly agreed otherwise.

4. PASSWORD

4.1 Usernames and temporary passwords will be issued upon account creation in line with Ridge's account creation procedure.
4.2 The provided temporary password shall be changed upon first logging in.
4.3 Passwords must meet the following requirements:
- Be at least 8 characters in length
- Contain at least 1 special, upper-case and lower-case characters.
- Not be identical to the last 3 passwords used.

4.4 Passwords must be kept secret and not divulged or shared with anyone, they shall not be written down and left anywhere that they can easily be found by someone else or recorded anywhere outside of a corporate password management system.
4.5 Users must not use the "Remember Me" functionality to store Ridge passwords on non-corporate devices.
4.6 Passwords must be changed if there is evidence of possible system or password compromise.
4.7 Different passwords must be used for organisational and personal use.
4.8 Upon user request to replace passwords will be administered to the user by RT Systems.
4.9 IT currently do not store any system or service level passwords which are required to be used by multiple Ridge members of staff or contractors.

5. SOFTWARE

5.1 There must be no attempts to over-ride any Ridge installed software, including anti-malware software, software firewalls and automatic updating services. If there is a valid business reason to do so authorisation must be obtained from IT and doing so must not introduce new vulnerabilities or malicious software into Ridge systems.

5.2 Users must not download or install any software for which Ridge does not have a valid license or is a threat to the organisation nature or would introduce vulnerabilities to Ridge systems (through for example, being out of support).

5.3 Messaging facilities shall only be used in a professional capacity, spam or malicious messaging, offensive or defamatory comments are prohibited.

5.4 Users must ensure that their workstation is always up to date, this includes the operating system as well as all software installed in the machine.

6. CLEAR DESK POLICY

6.1 Persons performing work under Ridge are required to ensure that no confidential information, whether in paper or other media such as USB's, is left on desks in work environments either within the office or a remote environment.

6.2 Information shall be retrieved from reproductive equipment, such as photocopiers or printers, as soon as possible and should not be left unattended. Furthermore, staff should consider whether any piece of reproductive equipment is suitable for the information being handled.

6.3 Confidential information shall be disposed of in line with Ridges Information Classification Policy when no longer needed.

6.4 Users must ensure that no one is able to access their workstation when they are not in attendance, to achieve this, users should lock their machines.

6.5 Any remote sessions to other physical or virtual machines must be terminated when no longer required.

7. BACKUPS

7.1 Users are responsible for ensuring that all important information is stored within Workspace or Ridges networked drives, unless that information has specific other requirements.

7.2 Users should refer to the Information and Classification Policy for guidance on where to store information of varying sensitivities.

7.3 Users should be aware that the availability of information stored solely on a local workstation cannot be guaranteed.

8. ASSET & MAINTENANCE

8.1 The user is responsible for the physical security and maintenance of their own workstation and any other assets that have been provided to them. Any faults or loss/theft of an asset should be reported to internal IT immediately.

8.2 Physical assets will be managed in line with Ridge's asset management procedures.

8.3 Assets should be disposed of in line with Ridge's disposal process and information classification system.

9. DATA HANDLING

9.1 When handling data or data bearing devices, users must conform to Ridges information classification policy, which details how various sensitivities of data should be, for example, stored, transmitted and disposed of.

9.2 Users must conform to any legal (e.g., GDPR and the Data Protection Act 2018) or contractual requirements (such as NDA's and information transfer agreements) as relevant to their roles.

10. AUDIT AND SECURITY MONITORING

10.1 Ridge deploys Lan Sweeper on all user devices, to manage and track corporate assets. Users shall not disable or remove this tool without express permission from IT.

10.2 Workstations are domain joined and should not be removed from the domain, without express permission from IT.

10.3 Reports of software contained on, and the configuration of workstations may be generated as part of internal checks and audits.

10.4 All activity taking place on Ridge networks or systems may be monitored to maintain the security of Ridge's operations.

11. REVOCATION AND CHANGE OF ACCESS RIGHTS

11.1 The revocation or change of access rights will be decided by Line Managers, or Heads of Departments/asset owners, who will affect these changes with internal IT.

11.2 Ridge has the right to change or revoke access rights to any corporate system, at any time, for any reason that aligns with the objective of maintaining information security and business continuity.

11.3 Upon changes to staff employment or work responsibilities, access rights will be reviewed and amended as required, to ensure they are suitable for any new roles and responsibilities.

12. EMAIL SECURITY

12.1 Organisational e-mail facilities may not be used for sending defamatory e-mails, or using e-mail for harassment, unauthorised purchases, or for publishing views and opinions (defamatory or otherwise) about Ridge, Employees, workers, suppliers, partners or customers of Waterstons.

12.2 Organisational e-mail may only be used for the communication of confidential information in line with the requirements of Ridges information classification policy.

12.3 Users must not disable the security built into their mail client that encrypts communication to and from the mail server.

12.4 Users must not open incoming e-mail attachments that originate with unknown third parties. These attachments may contain malware and any such e-mails must be reported to Internal IT immediately by email, telephone or in person, and on no account should they be forwarded to anyone.

12.5 Users must ensure that an appropriate Out of Office message is setup for the duration of any leave from work.

12.6 Ridge also retains the right to modify mailbox permissions when required for the following scenarios:

12.7 Adding/removing access to shared mailboxes or Send As permissions to reflect a change of job role or responsibilities

12.8 Granting another individual temporary access to the employees' mailbox if information is urgently required due to a critical business need, and they cannot provide this due to absence

13. REMOTE WORKING

13.1 Users can remotely access Ridge systems, but should do so strictly for business reasons only

13.2 The workstation must be physically secured from theft or eavesdropping/shoulder surfing, both at rest and in transit, and the physical security of the site must be considered by the user before working remotely – particularly in public places

13.3 The workstation must not be used to access Confidential or Restricted data while in a public place, or an environment in which unauthorised individuals can view the data.

13.4 Users that are provided with a Ridge workstation or laptop should adhere to the guidelines set out in section 15.

13.5 Remote access to Ridge systems is affected through the use of VPN.

13.6 All workstations used for remote access must have a fully licensed and updated antivirus and firewall always enabled.

13.7 Only the intended user can access the remote access session or Ridge information assets/systems – this must be enforced by the workstation having a password protected user account, by the user locking or shutting down the workstation when inactive and by closing remote access sessions when finished with them

13.8 Data should be only stored on the workstation and its associated removable media where its data classification allows, as in line with Ridge's information classification scheme, and with the appropriate security measures in place.

14. INTERNET ACCEPTABLE USE

14.1 Organisational User IDs, websites and e-mail accounts may be used both for organisationally sanctioned communications and personal communications, as long as these do not interfere with employment responsibilities.

14.2 Use of Internet/intranet/e-mail/instant messaging may be subject to monitoring for reasons of security and/or network management and users may have their usage of these resources subjected to limitations by Ridge.

14.3 The distribution of any information through the Internet (including by e-mail, instant messaging systems and any other computer-based systems) may be scrutinised by Ridge and Ridge reserves the right to determine the suitability of the information.

14.4 The use of organisational computer resources is subject to local law and any abuse will be dealt with appropriately.

14.5 Users may not visit Internet sites that contain obscene, hateful or other objectionable material, and shall not make or post indecent remarks, proposals or materials on the Internet.

14.6 Users may not upload, download, or otherwise transmit commercial software or any copyrighted materials belonging to the company or any third parties without a legal business case.

14.7 Users may not download software from the Internet or execute or accept any software programs or other code on the Internet unless it is in accordance with Ridge policies and procedures, and as specified in this policy.

14.8 Users will not intentionally interfere in the normal operation of the network or take any steps that substantially hinder others in their use of the network, and will not examine, change or use another person's files or any other information asset for which they don't have the Owner's explicit permission.

15. LAPTOP SECURITY

15.1 Ridge requires laptops to remain locked when not in use, to have BitLocker enabled at all times for the encryption of files, and to have a Lan Sweeper agent installed and at all times.

15.2 Users must report any technical issues to Internal IT, in particular issues affecting the security software or physical integrity of the laptop

15.3 Users are required to ensure that all the most recent operating system and application security-related patches, fixes and updates, as deployed by Ridge, have been applied to the workstation.

15.4 Users of laptops are required to not locally save data whose integrity and availability is key, and instead should use Ridge's network storage services.

15.5 Users are required to ensure that, when in transit, the laptop is carried as hand luggage, in its protective bag or an appropriate backpack and that, when it is not in use, it is not left unattended in public places. In cases of loss or theft of the laptop, they must report this to Internal IT immediately.

15.6 Users must act with care in public places so as to mitigate the risk of screens containing confidential information being overlooked by unauthorised persons.

15.7 Ridge provides Users with appropriate training and awareness to ensure that they understand the risks of working in public places and that they understand and can carry out their security obligations.

16. MOBILE PHONE SECURITY

16.1 All corporate data on mobile phones must backed up regularly to corporate storage, and removed when no longer required

16.2 Users must take care when using the mobile phone in public places, to avoid the risk of other people overhearing any conversation that might involve confidential information.

16.3 Users must apply operating system patches to mobile phones within two weeks after their release, unless advised otherwise by the Internal IT.

16.4 Users must protect my phone with a secure screen locking mechanism.

16.5 If the security of a corporate mobile is compromised via theft, loss or malware infection, users shall inform Internal IT immediately.