Data Classification: **CONFIDENTIAL**

Acceptable Use

Contents

Our Core Principles:

- Colleagues are trusted and respected to work responsibly in the best interests of customers and the Society
- Colleagues are empowered to make their work lives meaningful, fulfilling, and productive to stay happy and healthy
- Fairness and inclusivity guides everything we do
- We're open-minded and forward thinking – we listen, experiment, learn, adapt and change
- Everyone's trusted and expected to use the principles to guide their decisions, behaviours, and actions and to apply our policies fairly (which won't always mean equally).

Purpose:

The Acceptable Use Policy outlines your responsibilities when accessing the Society's information, using equipment and accessing any systems. It also includes guidance on our responsibilities to protect Society information in any of the physical locations we work.

Scope:

This Policy helps us embed our acceptable use principles, and applies to all Skipton Building Society, Skipton Business Finance and Jade colleagues, including all temporary agency staff, interns, students on work placement and anyone who is subcontracted to undertake specific duties for those organisations listed above

This policy is part of your contract of employment. We'll consult with Aegis on any changes to this policy.

Definitions:

Malware: software that's designed to disrupt, damage or gain unauthorised access to an IT system.

Policy Statement:

The world around us is changing and we're becoming more flexible in how we work. We live in a data-driven world and the equipment and systems we use to access, process and store information change all the time. Using information well makes our lives easier, more convenient and connected. But we must strike a balance when making sure our data, equipment and locations are accessible to those who need to use them, of also keeping things safe and secure to protect the Society, colleagues and our customers from the risk of information falling into the wrong hands.

Section 1: Our Society commitments

- We provide appropriate equipment and systems, so you can do your job well and Society, colleague and customer data is kept secure.
- We apply regular updates to systems to provide the latest features to keep things running securely and smoothly.
- Service Desk colleagues are available to help you use equipment and systems easily. They're there if you need to report any problems. They can be contacted on 01756 705018 during the following hours:
    - Monday to Thursday 8am – 6.30pm
    - Friday 8am – 6pm
    - Saturday 8.30am – 12.30pm
- We monitor all internal communication channels, equipment and systems to keep Society, customer and colleague data secure and to uphold our responsibilities as a regulated organisation. But, in line with our Society value of Trust, we only monitor what's strictly necessary and respect our colleagues' and customers' right to privacy.
- Any equipment or software is provided so you can do your role, but limited personal use is allowed, if your own use doesn't interfere with you doing your role or breach any Society policies or procedures.
- We make sure our workplace locations are designed to be accessible and to protect you, our equipment and information.

Section 2: Your Responsibilities

We all have a responsibility to use Society equipment and systems in line with this Policy. This helps keep our data and information secure so we meet the requirements of our Regulators, stay well within the law and live up to the expectations of our colleagues and customers.

Here's some things you're responsible for:

- Reporting any actual or suspected inappropriate use of Society information or equipment as soon as possible to the IT Service Desk on 01756 705018 or by email sscservicedesk@skipton.co.uk or to your Leader
- Thinking about who can see your screen and positioning it so sensitive information can't be read by others. If it's difficult to do this, you can request a privacy screen via the IT Service Desk. If you're working from home, be mindful that your screen could be visible to those you live with or even through a window.
- Keeping screens locked when away from your computer. When you're finished for the day, close down all applications and shut down your computer so any updates are installed correctly.
- Only ever accessing information connected with your role and never viewing information about people personally connected to you. If you find yourself required to access information about yourself, colleagues, friends or family as part of your role then please let your Leader know.
- When collecting, using, storing and sharing personal data we must adhere to key principles known as the data protection principles as outlined in the General Data Protection Regulation (GDPR). We must make sure personal data is:
    - used fairly, lawfully and transparently
    - used for specified, explicit purposes and not used in a manner incompatible with those purposes

    - adequate, relevant and limited to only what is necessary
    - accurate and, where necessary, kept up to date
    - kept for no longer than is necessary
    - handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage
- Only browsing network files and directories for work-related information. You should never access or try to access data where it's unrelated to your role. If you find you have access to information or systems that you don't need or which aren't relevant to yor role, speak to your Leader who'll arrange to remove the access.
- Contacting the IT Service Desk if you need to request any changes to your equipment - hardware or software.
- Frequently connecting your equipment to the Society's network to ensure you get all relevant software and security updates.
- Immediately contacting the IT Service Desk if you notice unusual activity which could be a malware infection or a security vulnerability. Never delete or remove the malware yourself or try to demonstrate that a weakness exists.
- Thinking about who can overhear your work conversations and those conversations outside the workplace when you're talking about work. You're representing the Society whether you're in a workplace, your home, a coffee shop or on a train. Be aware of who's around you if you're talking about work or sharing sensitive information.
- Remember your job comes first. Don't let personal calls, using the internet or checking your social media get in the way of doing your job.
- Maintaining a tidy desk wherever you're working and locking confidential documents containing customer, colleague or commercially sensitive information in a cupboard or drawer when not in use. When you leave your desk and at the end of the working day, put the key somewhere safe and secure. If you're hotdesking, leave the workstation as you'd wish to find it.
- Disposing of confidential papers using the confidential waste bins or the process you've got in your workplace. If you're a hybrid worker, never use your home bin. Bring your confidential waste with you on an 'in-office' day to dispose of securely.
- Keeping your password secure. Don't write it down or disclose any information to other colleagues to enable them to access your accounts. You're fully responsible for all activity carried out under your log-on.
- Never logging on for other colleagues. If you suspect your password has been compromised, you must change it immediately and report it to the IT Service Desk.
- Not sharing any of your system logon details with anyone. However, you may provide temporary access to your email account when it's required short-term for a work-related reason and your leader has agreed it. For example, this could mean setting up access for a colleague to check your inbox while you're on holiday.
- Enrolling onto the Password reset tool. This is the easiest way to reset a password if you become locked out of your account or forget your password.
- Storing company confidential data or personal data on department sharedrives so it's backed up and secure. If it is necessary to hold information temporarily on a local drive (i.e. your desktop), remove it immediately after you've finished with it.
- Being careful with what you put in emails as they can be legally binding. They can also be used in legal proceedings.
- Only signing up for mailing lists when they're genuinely useful for your role.
- Wearing a colleague pass or name badge when you're on Society premises.
- If any Society equipment is lost or stolen this should be reported as soon as possible to the IT Service Desk on 01756 705018 or by email sscservicedesk@skipton.co.uk who will then

remotely wipe the device and ensure our data remains secure. Any thefts should also be reported to the Police and the IT Service Desk will ask you for the crime reference number.
- Report any incidents, such as if you've clicked a link which doesn't look right or sent something to the wrong place, then contact IT Service Desk

Some key things to remember about your responsibilities:

Your responsibilities under this Policy don't stop at the office door or the end of the working day. If you knowingly misuse equipment or systems in ways that put the Society, our colleagues or customers at risk, we'll take this very seriously. We'll investigate it in line with the Disciplinary section of the Resolving Conflict Policy (Link coming soon).

The following activities are unacceptable in our workplaces:

- Downloading, creating, sharing, saving or sending:
    - any offensive, obscene or indecent images, data or other material,
    - unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which could be linked to radicalisation;
    - unsolicited Spam emails;
    - material which is subsequently used to facilitate harassment, bullying and/or victimisation of another person;
    - material which promotes discrimination on the basis of any protected characteristic (including race, gender, religion or belief, disability, age or sexual orientation);
    - material with the intent to defraud or which is likely to deceive another person;
    - material which advocates or promotes any unlawful act;
    - material that infringes the intellectual property rights or privacy rights of another person, or
    - material that brings the Society into disrepute.

- Carrying out any malicious activities; or intentionally or recklessly introduce any form of malware.
- Using Society systems, data or software for personal monetary interests or gain. This could be a criminal offence and lead to action being taken against the Society and you.
- Using recording devices in the workplace, including smart devices, (unless you've had prior agreement from your Senior Leader.
- Using Society systems to copy and/or transmit any documents, software or other information protected by copyright law without the appropriate licence or permission.

Section 3: Managing data

Society data includes any information about a customer, colleague, business transaction or other aspect of the Society held on paper or digitally. It includes our intellectual property (such as software code, designs and strategies) and information about our finances. It can be printed, in a spreadsheet, document, core system, email, notebook or other file and in databases. Society data must only ever be stored on Society systems unless you've got approval from Information Security to use a different service or system.

Our structured data is held in databases and means we can build rules around its safe storage and deletion. We still have lots of unstructured data which sits in areas outside of our controlled databases, such as department drives, emails, desktops, paper records and so on. The nature of these varied data sources means that it is much more difficult to put business rules in place around the data, and so we rely on individual areas across the Society to process, manage and delete their unstructured data locally, according to requirements set out in relevant documentation such as the Unstructured Data Framework, End User Development Standard (for if the data is used as part of a digital solution e.g. a spreadsheet used for reporting), Data Retention Policy and Framework.

Some key things to remember about managing data:

- Some data is classified as 'Confidential' or 'Restricted' so you'll need to take extra steps to keep it safe and secure. If you'd like to know more, take a look at the Data Classification Standard.
- Where information contains personal data, you'll need to it make sure it's processed in line with the Data Protection Policy.
- Cardholder data, in its entirety, must never be stored in electronic or paper formats. This includes the full Primary Account Number (PAN) which can be found on the front of payment cards, as well as the Card Verification Value (CVV) code which is the 3- or 4-digit numbers on the signature panel on the reverse of the payment card.
- If you create unstructured data, you're responsible for deleting it too! Creating unstructured data happens any time you take data from a core system and save it somewhere else, such as in an email, or written in your notebook.

Section 4: Communication

Communication is the act of transferring information from one person, place or group to another. It sounds simple doesn't it? Effective communication, however, is about more than just exchanging information. It's about sharing the emotion and intentions behind the information and is a huge part of us working well together. If you're interested in developing skills to help you communicate more effectively, we've plenty of resources available. We have different channels available to help you share information and here's a few details about each of them.

Emails

External emails (that come to you from outside of the Society or that you send outside of the Society) are not secure, Emails can be intercepted and read while it's being sent from one person to another . If you're sending any information you've classified as 'Restricted' or 'Confidential' by email, add the word **$ecure** at the start of the subject line to keep it secure.

Some key things to remember about emails:

- Never send any payment card or cardholder information in an email whether this belongs to a customer, a colleague or you.
- Don't open any links or attachments in an email unless you're confident it comes from a genuine source. If in doubt, contact the IT Service Desk.
- Never use a personal or non-Skipton email account for Society business, and Society emails mustn't be automatically forwarded to a non-Skipton address.

- You mustn't send work to a personal email address or a personal device (including to home printers) without permission from your Leader.
- If you use your work email account to send personal emails, everything outlined in this policy still applies. –Remember that a personal email sent from a business account could be construed as Society business, opinion or professional advice, so be careful what you write.
- You're responsible for all emails sent from your account. So read things carefully before you create or forward an email and check the attachment is the one you intended to send. Check the recipients details carefully especially when it's a more common name. If you send an email in error, you should attempt to recall it immediately (if it's been sent internally).
- If an email containing personal data is sent to the wrong person even if it's by mistake, it could be deemed a data breach and must be reported to the IT Service Desk straight away.

Online meetings and conferences:

Most of us are really familiar with online meeting technology (such as Microsoft (MS) Teams and Zoom) and they're an effective and productive way to meet and work together, especially when we're working with others in different locations. When you're working with external third-parties, there are some extra steps to think about, so you keep our systems and information secure. Remember, if it's your meeting, it's your responsibility to manage any data in line with our Policies and data regulations.

Some key things to remember when using online meeting systems:

- Only use software that's approved by the Society, such as MS Teams.
- It sounds obvious, but make sure you know who you're talking to.
- You're responsible for the meeting, so only share information with a third-party if there's a good reason to do so. You might need prior authorisation from the Information Security team, but if in doubt about what to share, check with your Leader.
- Don't share any Confidential or Restricted documents, or any customer data with external third-party participants, unless this has been agreed with your senior Leader.
- If you record meetings with third-parties make sure that you've confirmed that it's ok with them to do so. These recordings shouldn't be shared with anyone else outside of Skipton and should be classified as 'Restricted' so that only the relevant people can view them.
- In exceptional circumstance that you need an external third-party to remote control or take control of a system, you'll need prior authorisation from the Information Security team. Third-parties should always be 'chaperoned' when on our systems. You must never allow an external third-party to install any software to allow them access to our systems.
- Be aware of what's in the background when you're in an online meeting and consider blurring your background. Make sure that your screen can only be seen by people who have access to that information.
- Make sure that external participants leave the call before you do, to make sure the meeting has closed.

Instant messaging (i.e. MS Teams chat):

This is a great way to quickly connect to exchange ideas and information. Instant messaging is very informal, but still needs using responsibly. Never write anything in instant messaging that you wouldn't say to someone in person.

It's not a suitable channel for capturing or sharing information about customers or colleagues that we'd want to keep on record or for documenting or recording any Society decisions.

Internet Use:

We use the internet regularly to find information, network with others and access third-party websites, however not all websites and online services are safe or authorised for use, even if you can access them through the Society's network.

The internet is made up of many types of media and new developments are taking place all the time. Our Information Security team share ways to keep your own and Society information secure when online, so make sure you keep up to date with your knowledge.

We encourage you to share your passion for working at the Society through social media if what you're sharing is accurate, framed respectfully and doesn't breach any part of our Policies.

It's really important that any posts that talk about our products and services are shared from verified Society sources, so you don't breach any financial promotions regulation. There's more information about ways to responsibly use social media in our Social Media Policy.

Some key things to remember when using the internet and social media:

- You should only join online forums, discussion groups and other similar facilities when they're legitimately required for your role.
- You must never download or install software from the internet onto Society systems unless it's part of the role you are trained to do e.g. IT Desktop Support Specialists
- 'Confidential' or 'Restricted' Society information must not be posted on the internet, unless it's part of your role to communicate information in this way
- You must never share any customer or colleague personal data over the internet or on social media unless this is part of your role with us

Section 5: Hardware, Software and remote connections

You'll be provided with appropriate equipment and systems to do your role. If you need any additional equipment or software or you need an workplace assessment to help you get the right adjusted equipment in place (to support you with a disability or underlying condition), there's help available.

If you're finding it difficult to connect from a remote work location, then the IT Service Desk will guide you. However, the IT Service Desk won't be able to help with any queries about your home broadband or Wi-Fi, questions of this nature should be directed to your broadband provider.

Personal devices:

We're working towards having more systems you can access from your own personal devices to give you more flexibility and the convenience of having fewer systems to configure to your personal needs. We'll update our guidance to ensure that you know what you can and can't access and how to work securely, whichever device you're using.

If you're approved to use your personal device, we expect that you'll take the same care as you would with any Society owned equipment. We expect you to adhere to password best practice, ensure your personal device is not left unlocked in a public place, use multi-factor authentication, where appropriate, and log out of any systems/applications promptly when you have finished viewing each time.

Remote Connections:

You must always use the Society's approved remote access software to connect to the Society network when you're working away from the office. You'll need to connect to get access to your usual systems and applications, and to access the internet. Connecting to the network means our information is protected. You're encouraged to follow all the good practice guidelines that we adopt in the Society for your home router too. Having password protection in place on your home Wi-Fi helps keep your personal information secure and when so much of our lives is carried out online, is a good habit to get into.

If you need third-parties to access our systems remotely, you'll need prior approval from the Information Security Team. You must never attempt to connect to Society systems from outside the network unless you are using an approved method.

Hardware and Software:

You must only change the Society's IT systems if it's part of your role and you've had the right training to allow you to do it properly (…and always use a change control procedure).

If you require any new IT or Technology services, including computer hardware, software and associated services, then this must be requested through the IT department. This means we get the best solution for our budget and we'll make sure it works well alongside the rest of our IT infrastructure. This includes any cloud or Software as a Service (SaaS) solution.

If you need any additional software to do your role, you must submit a request to IT and if approved, IT will carry out the installation. If you spot any unauthorised or suspicious software on your equipment, report this immediately to the IT Service Desk.

You must not copy software and other forms of intellectual property for personal use or use in violation of licence agreements.

All IT equipment must be disposed of carefully and by the IT Service Desk, in line with the agreed processes.

Some key things to remember when using hardware, software or connecting remotely:

- You must never load, download, install or store unapproved, unlicensed or unauthorised software or applications from any source, including the internet, on Society equipment. If any unauthorised or illegal software is discovered on Society equipment, it'll be removed without notice.
- External USB charged devices such as e-cigarettes or smartphones can affect our systems, so must never be connected to Society equipment.
- You can use the Society Colleague Wi-Fi network when using any personal devices in our workplaces.

Section 6: Physical Security

Working Flexibly gives us more choice in where we work, but when we're moving between different locations there's an increased risk of leaving equipment and/or information unattended, or even leaving items behind. You're responsible for the equipment you've been issued and for protecting it, (along with our data) from theft, abuse, damage or unauthorised use at all times. Essential business-related items are covered by the Society's insurance policy, but of course it's your responsibility to make sure you don't do anything which could invalidate the insurance.

Some key things to remember about physical security:

- If you're travelling for work, you may temporarily lock any paperwork or equipment in the boot of the vehicle, providing it's not visible from outside.
- You must not store paperwork, laptops or other mobile computing devices in a vehicle for a long period or overnight.
- You must not leave Society equipment or information unattended in public.
- If you need to move any Society equipment around our workplaces such as desktops, monitors and docking stations you must request this from the IT Service Desk, so they're able to keep track where everything is! You can of course use your portable equipment (laptops, tablets etc) in any agreed location.
- When you're in the workplace, portable equipment, such as laptops should be out of sight and secure when not in use
- If you have Society equipment at home, you must follow sensible home security steps such as locking windows and doors when you're away from your property and not leaving valuable equipment in view to passers-by.
- If you're working from home, be sure to store equipment and information out of view from others when you've finished working
- If you're using your equipment from home, it's for your use only and not for family, friends or visitors to use.
- Where possible, and especially when you're working from home, you should aim to work 'paperless'. If you do need to take documents home to read, remember the data classification and store them accordingly. When you've finished with them, they should be returned to the workplace and disposed as confidential waste.
- If you're working at Head Office, you'll need a colleague or a temporary pass to get round the building and use some of the equipment.
- If you invite a visitor to any of our workplaces, they'll need a chaperone while they're in the building.

Section 7: If you need further support:

Remember we have the IT Service Desk team (01756 705018) and our Information Security team are on hand to help.

Section 8: And here's the housekeeping bit;

Communication:	This policy is available to all colleagues through Connect
Implementation:	Mandatory learning modules, Connect articles, one to one conversations.
Evaluation:	Data security breaches, mandatory training uptake and outcomes, Employee Relations themes.

Related policies	Working Flexibly, Social Media, Data Protection, Resolving Conflict
Related guidance	Data Protection, Colleague data privacy notice, SBS Password Reset, Unstructured Data Framework, End User Development Standard Data Retention Policy, Data Retention Framework, Data Classification Standard, Social Media Policy, Additional equipment or software request
Policy Owner	People Team and Information Security
Last Updated	June 2022
Approved by	Information Security Policy Review Group, Data Governance Group
Frequency of Review / Approval	Annual

Contact the People team if you'd like details of any previous versions of this policy