Information Systems – Appropriate Use Policy

Purpose	The purpose of this policy is to outline the appropriate use of information, computer and communication systems at Asahi UK and Asahi Europe Ltd. These rules are in place to protect the users (see scope below) and the company. Inappropriate use exposes the Company to risks which can compromise the confidentiality, integrity and availability of information.
Scope	All Users of Asahi UK and Asahi Europe networks, communications or computing resources. Users are defined as all Asahi UK and Asahi Europe employees, consultants and contractors.
Principles	The Company's information and computer systems are assets critical to the conduct of the Company's business and stakeholders, and its dependency on these assets demands that appropriate levels of information security be instituted and maintained. It is the Company's policy that appropriate measures are taken to protect its information and computer systems against accidental or malicious destruction, damage, modification or disclosure, and to maintain appropriate levels of confidentiality, integrity and availability of such information and/or company computer systems. Users of the Company's networks or computing resources should be aware of the risks involving information stored electronically in order to take the necessary precautions to ensure these risks are mitigated. The following are the main risks relating to information of which users should be aware: • Disclosure of sensitive[1] business or personal information; • Inadvertent or deliberate deletion or change of information; • Unavailability of information.
Accountability	The HR Department and the IT department are responsible for issuing and updating this policy as necessary to comply with regulations and applicable Company policies. It is the responsibility of all employees, consultants and contractors to ensure they are fully aware of company policies and that they are acting in accordance with those policies. Line Managers and the HR Department have responsibility for monitoring compliance with the policy. Failure to comply with this policy may result in disciplinary action being taken against the user under the Company's disciplinary procedures, which may, depending on the circumstances, include the withdrawal of permission to use the company's equipment for personal purposes and/or a formal written warning or summary dismissal. The confidentiality clause in your employment contract applies to any online activity that you undertake in your personal time. You may not disclose any sensitive or proprietary information about the company or its employees. You may face disciplinary or even legal action if you disclose information of a sensitive nature. Defamatory reference made to The Company, its staff or suppliers in a personal blog or on any other social media platform could result in disciplinary action under the Company's Disciplinary Policy. Please also be aware that engaging in online activity, whether in your own right or as a company spokesperson may attract media interest in you as an individual, so proceed with care whether you are participating in an official or a personal capacity. If you have any doubts, take advice from your line manager.
Contact	For further advice relating to the above information or other policies, please contact a member of HR or IT team at the Woking office.

Note: This policy does not form part of the contract of employment; however, the Company will not depart from it without good reason.

Policy	
1.	**Computer usage - in office and general use**
	• Many aspects of communication are protected by intellectual property rights which are infringed by copying data. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or of other intellectual property rights. Users must not download or distribute pirated software or data. Any software or files downloaded may only be used in a manner consistent with their licences or copyrights. If in doubt users should contact the IT help-desk before downloading any material. • Users must not generate, upload, access, download or distribute any material that could be deemed pornographic, racist, sexist, homophobic or otherwise offensive. The display of any offensive or sexually explicit image or document on a Company system is expressly prohibited. In addition, offensive or sexually explicit content may not be archived, stored, distributed, edited or recorded on Company's network or computer resources. • Users must not seek to gain access to restricted areas of the network or access or try to access data which they know or ought to know is sensitive. • Users must not attempt to probe, scan or breach the security or authentication measures of a system or network either internally or externally using Company resources. • Users must not knowingly propagate any virus, worm, Trojan horse, trap-door program, or similar code. If such virus, worm, Trojan horse, trap-door program or similar code is discovered by a user, he/she must cease using the system immediately and report the discovery to the IT help-desk. • Users must notify the helpdesk if any of their visitors are required to connect a non Company computer or device to the network so that it can be checked to ensure it is appropriately updated and free of viruses. • Users must not install unauthorised hardware or software. • Users must not knowingly disable or overload any computer network, or circumvent any system intended to protect the privacy or security of another user. • Users shall not knowingly allow the use of their username and/or password by anyone else, whether such other person is an authorised user or not. Users are accountable for all activities carried out under their username and password. • Users must not possess tools, software or code, (including packet-sniffing or password-detecting software) which enables a user to circumvent the security of a computer system. • Users are required to ensure that all data that may be required to be retained by applicable legislation or in terms of the Company's document retention policies as communicated to them, is retained and stored in compliance with such legislation or policies. • Users must take adequate steps to protect the physical security of the computing resources within their possession by ensuring portable devices are securely stored when not in use and workstations are locked when left unattended. Passwords must be kept confidential. • Breach of the provisions above would not only contravene the terms of this policy but may also lead to an offence under the Computer Misuse Act 1990, which creates the following offences: o unauthorised access to computer material i.e. hacking; o unauthorised modification of computer material; o unauthorised access with intent to commit or facilitate the commission of further offences.

2.	**Computer usage – home & remote working**
	• Users provided with the Company's computing resources for home or remote use must take additional precautions to ensure the confidentiality and integrity of Company information by: o ensuring mobile devices including laptops and PDA's are adequately secured and not left in places where they are visible to passers by e.g. cars; o ensuring Company resources are not used by non Company personnel; o ensuring that sensitive information is not inadvertently viewed by third parties (e.g. use of laptops on public transport or airport lounges); o complying with all aspects of this policy.
Guidelines	• Always lock your PC before leaving it unattended by pressing 'CTL ALT DEL enter' or 'Windows key L'. • Set an Outlook reminder to change your passwords regularly, then you can keep your passwords synchronised and you're less likely to forget them. • An example of how to choose a strong password – Choose a memorable phrase and use the first letter of each word as your password. You can also incorporate upper and lower case letters, numbers and special characters. e.g. I go home at 17:30 becomes **Igh@17:30** • The Post-It note with the password written on it stuck to your PC is really not a good idea! • Transport your laptop in the boot of your car. That way if you have to leave the car unattended your laptop will be secure and out of sight. • Ensure you store any access token separately from your laptop. That way if the worst happens and your laptop gets stolen the thieves will not have the token to gain access to the corporate network. • Report any theft or loss to the IT department immediately
3.	**Electronic email & messaging Systems – business use**
	• Users must take particular care when using e-mail, or social media as a means of communication because all expressions of fact, intention and opinion may bind the user and/or Company and can be produced in court in the same way as other kinds of written statements. • Users must only use the corporate approved instant messaging system for quick transitory messages similar to a quick phone call or a quick in-person verbal communication. • Users must not use the corporate approved instant messaging system for transmitting substantive business or sensitive personal information as these messages are not retained or saved. • Any substantive transfer or recording of substantive business records or information must be done via a non-transitory means such as a memorandum, other acceptable business record medium or, at the very least, with an e-mail message. • Users must not send, or post, messages or files, which could be construed as defamatory, harassing or otherwise offensive. This includes the use of profanity, obscenities or derogatory remarks relating to employees, customers, suppliers or others. • Users must take reasonable precautions to advise senders not to send inappropriate emails to the users company email address. • Users must not send sensitive information over the internet without adequate protection. • Users of Company's e-mail and messaging systems must not knowingly distribute or forward hoax virus warnings, chain letters or unsolicited mail of any

	kind. • Users must not access any other person's in-box or other e-mail folders nor send any email purporting to come from another person without explicit authorisation from that person e.g. through Outlook delegates. • In light of the security risks inherent in web-based e-mail accounts such as Yahoo and Hotmail, users must not e-mail business documents to their personal web-based accounts. Users should also not email sensitive documentation to their home email accounts. If files need to be accessed from home the User should apply for access to the approved remote access solution.
4.	**Electronic email & messaging systems – personal & general use**
	• Although Company's e-mail facilities are provided for business purposes, it is accepted that users may occasionally use them for their own personal purposes. This is permitted on the condition that all the procedures and rules set out in this policy are complied with. Users should be aware, however, that if they choose to make use of these facilities for personal correspondence, they can expect limited privacy because the Company may need to monitor communications for the reasons given in the procedure section of this document. • Under no circumstances may Company's facilities be used in connection with the operation or management of any business other than that of Company. • Users may use public instant messaging systems for personal communications to communicate with known trusted correspondents i.e. communication with anyone not in the contact/buddy list must be blocked. • Users must ensure that their personal e-mail and messaging use: o does not interfere with the performance of their duties; o does not take priority over their work responsibilities; o does not cause unwarranted expense or liability to be incurred by the Company; o does not have a negative impact on the Company in any way; o is lawful and complies with this policy; and o is not excessive. • Users must be aware that any correspondence made using Company's electronic facilities (including personal email) may have been copied onto backup tapes and retained indefinitely. • By making personal use of these facilities the user signifies their agreement to abide by the conditions imposed for their use, and signify their consent to the Company monitoring their personal e-mail and messages in accordance with the procedure section of this document.
Guidelines	• Exercise caution when using your company e-mail address to join networking sites. Whilst it may be appropriate to use this address for some (e.g. Linked-In), for others this may not be the case. Remember, your Company e-mail address has been provided for work purposes. • Be careful when you send e-mails of a personal nature (i.e. not directly related to your job as an Asahi employee) from your Company e-mail address, and to whom you send them. Information contained in your e-mails could be construed as coming from the company or representing it, despite the disclaimer text contained at the bottom of all company e-mails. • Always check the content of your message, the recipient's name and address before sending. • Consider that improper messages could make you personally liable or create liability for the company. • Remember that your e-mails are not private or secure. They are regularly monitored by the company and are easily accessed by others. • Think carefully before using the "Reply to all" function. • Don't ever send defamatory, sexist, racist or criminal material by e-mail.

	• Don't send it if in doubt. Remember that you do have a telephone.
5.	**Internet and intranet access and browsing – business use**
	• When visiting an internet site, information identifying a user's PC may be logged. Therefore any activity users engage in via the internet may reflect upon the Company. • Users must not access inappropriate websites, blogs, discussion forums or chat rooms, which have content that could be construed as defamatory, harassing or otherwise offensive. • Whenever users access a web site, they must always comply with the terms and conditions governing its use. • Users should be aware that the Company routinely blocks access to websites which are deemed to be inappropriate or impacting network performance, and any attempts to access such sites may be monitored and recorded. • Do not discuss sensitive aspects of your work, the Company or your colleagues in public blogs, wikis or social media platforms that could bring the Company into disrepute. Explicit or anonymous references to the organisation or its employees are not permitted.
6.	**Internet and Intranet access and browsing – personal & general use**
	• The Company recognises the need for individuals to have to carry out some personal tasks during working hours, e.g. for internet banking or on-line shopping, and this is permitted subject to the same rules as are set out for personal e-mail use in section 4 of this policy, • Users are strongly discouraged from providing their Company e-mail address when using public web sites for non-business purposes, such as on-line shopping. This must be kept to a minimum and done only where necessary, as it may result in the user and the Company receiving substantial amounts of unsolicited e-mail. • Do not place photographs of yourself, colleagues or friends which might be considered unacceptable in accordance with the responsible alcohol consumption policy on websites or social media platforms. It is important to familiarise yourself with the appropriate behaviour guidelines in the Company Alcohol Policy.
Guidelines	**General Guidelines** • Be wary of any pop ups on websites which ask you to download files. You may be inadvertently downloading malicious programs or spyware. Always check with the helpdesk if you are uncertain. **Social Media Sites** • Social media may be defined as: *Web-based applications, platforms and media which facilitate interaction, collaboration and sharing of content.*[2] At the present time, social media types of relevance to our business include: blogging, microblogging, wikis, discussion forums, networking, filesharing and bookmarking. • With any social media interaction, you must be mindful of, and clear about, the capacity in which you are engaging. Only trained Company spokespeople should make statements on behalf of our businesses or brands. If you are not a designated and approved spokesperson for your company in the traditional media, you should not be acting as one in the social media space. • Any employee engaging in social media on behalf of a business or brand should first refer to the Company *Social media guidelines for media relations* and the Company *Social media guidelines for brand communications*. Or the local versions of these documents.

	• If acting in a personal capacity, you should be mindful of your online conduct and its potential impact, especially if you have listed the Company as your employer. Even if you haven't mentioned Company, in an ever connected world, your association with the business may be considered public knowledge. • Information posted on social networking sites can have far-reaching consequences for individuals and the Company. All expressions of fact, intention and opinion may bind the user and/or the Company and can be produced in court in the same way as other kinds of written statements. Any online contribution by an employee which damages the Company's reputation may result in disciplinary action under the Company's Managing Poor Performance and Conduct Policy. • Think carefully about the amount and type of information you reveal in your online profiles, don't reveal details that should not already be public. Consider restricting access to your profile using the sites privacy settings where available.
Procedure	**Monitoring of communications and public domain**
	• The Company is ultimately responsible for all business communications but subject to that will, so far as possible and appropriate, respect the user's privacy and autonomy while working. The Company may monitor a user's electronic communications for reasons which include: o providing evidence of business transactions; o ensuring that the Company's business procedures, policies and contracts with staff are adhered to; o complying with any legal obligations, ethical codes and best practice; o preventing, detecting or investigating unauthorised use of the Company's communications systems or criminal activities; and o maintaining the effective operation of the Company's communication systems. • Users must be aware that the Company may monitor all messaging and internet traffic data (covering both personal and business communications) for the purposes specified above. Users must also be aware that such monitoring might reveal sensitive personal data about them. For example, if users regularly visit web sites which detail the activities of a particular political party or religious group, then those visits might indicate the user's political opinions or religious beliefs. By carrying out such activities using the Company's facilities the user consents to our processing any sensitive personal data which may be revealed by such monitoring. • Sometimes it is necessary for the Company to access a user's business communications during their absence, such as when the user is away due to illness or leave. Unless the user's mailbox settings are such that the individuals who need to do this already have permission to view their inbox, access will be granted only with the permission of their line manager and a member of Information Security. • Any e-mails which are stored in a user's mailbox and which are not marked PERSONAL in the subject heading, or which, from the description in the subject heading are not obviously of a personal nature, will be treated as business communications. It is up to each individual to prevent the inadvertent disclosure of the content of personal e-mail by clearly identifying it as such in the subject header. • In certain very limited circumstances the Company may, subject to compliance with any legal requirements, access personal email. Examples are when we have reasonable suspicion that they may reveal evidence of unlawful activity, including instances where there may be a breach of a contract with the Company or a Company policy. • Users must be aware that Company monitors the appearance and any potential misuse of the Company corporate brand name and associated company, product brand names in the online public domain.