Internet Acceptable Use Policy

Version 5, September 2021

The AS&K Group includes all associated companies and subsidiaries, and will be referred to as the Company herein.

Introduction

The *internet acceptable use policy* describes our rules, requirements and standards for use of the Company's internet and other electronic communications facilities. It should be read in conjunction with our policies on Social Media, Data Protection, and Information Security.

The Company Internet and communications facilities are made available to users for the purposes of the business. A certain amount of limited and responsible personal use by users is also permitted. All use of our communications facilities is governed by the terms of this policy.

Although the detailed discussion here is limited to use of internet, email and video conferencing facilities, the general principles underlying all parts of this policy apply to all communication devices and their use, not limited to telephones and mobile phones, fax machines, copiers and scanners.

Subject as set out below, you may use the Internet and your computer as you please provided that what you do is lawful, does not interfere with the proper performance of your employment duties, and is in accordance with this Policy and the Information Security, Social Media, and Data Protection Policies

Communications sent by you can have significant implications for the Company. In particular, the Company may be liable for your actions. It is therefore vital that you comply strictly with the terms of this Policy.

This Policy forms part of your contract of employment and breach of the Policy may lead to disciplinary action and, in serious cases, may entitle the Company to terminate your employment.

1. General Principles

1.1 You must use the Company's IT and communications facilities professionally, lawfully, consistently with your duties, with respect for your colleagues and for the Company and in accordance with this policy and the Company's other rules and procedures.

1.2 All information relating to our clients and contacts and to our business operations is confidential. You must treat our paper-based and electronic information with utmost care.

1.3 Internet access is provided primarily for business use. Limited and responsible personal use is permitted. Automated reports on daily usage currently flag substantially above average users, especially of non-business related sites.

1.4 Many aspects of accessible websites are protected by intellectual property rights that are infringed by copying. Downloading, uploading, posting, copying, possessing, processing and distributing material from the Internet may be an infringement of copyright or of other intellectual property rights.

1.5 Particular care must be taken when using email as a means of communication because all expressions of fact, intention and opinion in an email may bind you and/or the Company and can be produced in court in the same way as other kinds of written statements.

1.6 The advantage of the Internet and email is that they are extremely easy and informal ways of accessing and disseminating information, but this means that it is also easy to send out ill-considered statements. Messages sent on email systems or over the Internet should display the same professionalism you would apply when writing a letter. You must not use these media to do or say anything that would be subject to disciplinary or legal action in any other context, such as sending any discriminatory (on the grounds of a person's sex, race, age, sexual orientation, religion or belief), defamatory or other unlawful material. If you are in doubt about a course of action, take advice from your line manager.

2. Use of the Internet

2.1 We trust you to use the Internet sensibly. Bear in mind at all times that, when visiting a web site, information identifying your device may be logged; therefore any activity you engage in via the Internet may affect the Company.

2.2 Whenever you access a web site, you should always comply with the terms and conditions governing its use.

2.3 We recognise everyone's need to use the Company internet facilities to perform personal tasks during working hours, e.g. for internet banking or online shopping, and this is permitted. However, the Company's internet gateway is monitored. Automated reports on daily usage currently flag significantly above average users. Once your internet usage is flagged, your usage logs may be scrutinised and provided to your line manager.

2.4 You must ensure that your personal internet use:

- 2.4.1 does not interfere with the performance of your duties;
- 2.4.2 does not take priority over your work responsibilities;
- 2.4.3 is minimal and limited to taking place substantially outside normal working hours (i.e. during your lunch hour or before or after your normal hours of work);
- 2.4.4 does not cause unwarranted expense or liability to be incurred by the Company;
- 2.4.5 does not have a negative impact on the Company in any way; and is lawful and complies with this policy

2.5 You must not:

- 2.5.1 use any images, text or material that are copyright-protected, other than in accordance with the terms of the licence under which you were permitted to download them;
- 2.5.2 seek to gain access to restricted areas of the Company's network;
- 2.5.3 access or try to access data that you know or ought to know are confidential;

2.6 For your information, breach of these provisions for computer use would not only contravene the terms of this policy but may also amount to the commission of an offence under the Computer Misuse Act 1990.

3. Use of Email

3.1 Generally:

3.1.1 Always use the email template that contains the appropriate notice from the Company and do not amend this notice in any way.

3.1.2 Do not amend any messages received, and, except where specifically authorised by the other person, do not access any other person's inbox or other email folders nor send any email purporting to come from another person, unless authorised to do so by a Director.

3.1.3 If you copy an email to others, it may breach the Data Protection Act (2018) if it reveals all recipients' email addresses to each recipient (e.g. in the case of marketing mailing lists). It can also breach duties of confidentiality (e.g. in the case of internal emails to members of a staff benefit scheme). Accordingly, it may be appropriate to use the 'Bcc' (blind carbon copy) field instead of the 'Cc' (carbon copy) field when addressing an email. If in doubt, seek advice from your line manager.

3.2 Business use

3.2.1 Expressly agree with the customer/client that the use of email is an acceptable form of communication, bearing in mind that if the material is confidential, privileged or commercially sensitive, then unencrypted email is not secure. Encryption software is available; request assistance from IT Support if you judge that encryption would be appropriate.

3.2.2 Each business email must include the Company business reference.

3.2.3 If the email message or attachment contains information that is time-critical, bear in mind that an email is not necessarily an instant communication and consider whether it is the most appropriate means of communication.

3.2.4 You must not email business documents to or from your personal email account. You may send documents to a client's personal email account if you have the client's express written permission to do so. However, under no circumstances should you send any business sensitive or confidential documents to a client's personal email account, even if the client asks you to do so.

3.3 Personal use

3.3.1 Although the Company's email facilities are provided for the purposes of our business, we accept that you may occasionally want to use them for your own personal purposes. This is permitted on condition that all the procedures and rules set out in this policy are complied with. Be aware, however, that if you choose to make use of our facilities for personal correspondence, you can expect very little privacy because the Company may need to monitor communications for the reasons given in paragraph 6.1. You will greatly increase the privacy of any personal email by complying with the procedures set out in item 3.3.3.

3.3.2 Under no circumstances may the Company's facilities be used in connection with the operation or management of any business other than that of the Company or a client of the Company.

3.3.3 You may use your Company email address for personal correspondence, but these should be marked PERSONAL in the subject line and moved to a folder labelled 'Personal' on sending/receiving. You can set up rules in Outlook to do this automatically. Ask IT for assistance if needed.

3.3.4 As with any correspondence made using the Company's electronic facilities, you can delete personal email from the live system, but they will have been copied into backup and in that form will be retained for several years per our data retention policies.

3.3.5 By making personal use of our facilities for sending and receiving email you signify your agreement to abide by the conditions imposed for their use, and signify your consent to the Company monitoring your personal email in accordance with paragraph 6 of this policy.

4. Use Of Equipment And Systems

4.1 Misuse or abuse of our telephone, email, web conferencing software or Internet sites in breach of this policy will be dealt with in accordance with our disciplinary procedure. In particular, this covers inappropriate use by viewing, accessing, transmitting, posting, downloading or uploading any of the following material, or using any of the following facilities (this list is not exhaustive):

4.1.1 pornographic material; or

4.1.2 offensive, obscene, or criminal material or material that is liable to cause embarrassment to the Company and any of its staff or its customers/clients; or

4.1.3 a false and defamatory statement about any person or organisation; or

4.1.4 material that is discriminatory, offensive, derogatory or may cause embarrassment to the Company or others;

4.1.5 confidential information about the Company and any of its staff or customers/clients;

4.1.6 any other statement that is likely to create any liability (whether criminal or civil, and whether for you or the Company); or

4.1.7 material in breach of copyright; or

4.1.8 online gambling; or

4.1.9 making unauthorised copies of any software loaded on your computer; and

4.1.10 only download, upload or transmit materials via the Internet if you have an express or implied licence (permission) to do so;

4.1.11 sending or receiving illegal software via the Internet;

Any such action will be treated very seriously as gross misconduct and may result in summary dismissal. Where there is evidence of misuse, the Company is likely to undertake a more detailed investigation in accordance with its disciplinary procedures.

5. System Security

5.1 Security of our IT systems is covered in more detail in our *Information Security Policy*. We owe a duty to all of our customers/clients to ensure that all of our business transactions are kept confidential. If at any time we need to rely in court on any information that has been stored or processed using our IT systems, it is essential that we are able to demonstrate the integrity of those systems. Every time you use the system, you take responsibility for the security implications of what you are doing.

5.2 the Company's system or equipment must not be used in any way that may cause damage or overloading or that may affect its performance or that of the internal or external network.

5.3 Keep all confidential information secure, use it only for the purposes intended and do not disclose it to any unauthorised third party.

5.4 Keep your system password safe. Do not disclose it to anyone. Those who have a legitimate reason to access another user's email must be given permission from that other user and IT will provide guidance on how to do this.

5.5 If a document is sensitive or confidential, it should be stored in access-restricted areas of SharePoint, limited to those who should appropriately have access. IT can help setting up such areas. For highly sensitive documents, you should mark them as "private" and password-protect the document itself.

5.6 Copies of confidential information should be printed out only as necessary, retrieved from the printer immediately, and stored or destroyed in an appropriate manner. See also our *Data Protection Policy*.

6. Monitoring of Communications by the Company

6.1 The Company is ultimately responsible for all business communications but subject to that will, so far as possible and appropriate, respect your privacy and autonomy while working. However, the Company may monitor your business communications for reasons that include:

6.1.1 providing evidence of business transactions;

6.1.2 ensuring that the Company's business procedures, policies and contracts with staff are adhered to;

6.1.3 complying with any legal obligations;

6.1.4 monitoring standards of service, staff performance, and for staff training;

6.1.5 preventing or detecting unauthorised use of the Company's communications systems, or criminal activities; and

6.1.6 maintaining the effective operation of the Company's communication systems.

6.2 The Company will monitor telephone, email and internet traffic data (i.e. sender, receiver, subject; non-business attachments to email, numbers called and duration of calls; domain names of web sites visited, duration of visits, and non-business files downloaded from the Internet) at a network level (but covering both personal and business communications) for the purposes specified at item 6.1. For the purposes of maintenance of your own personal privacy,

you need to be aware that such monitoring might reveal sensitive personal data about you. For example, if you regularly visit web sites which detail the activities of a particular political party or religious group, then those visits might indicate your political opinions or religious beliefs. By carrying out such activities whilst using the Company's facilities, you consent to our processing any sensitive personal data about you that may be revealed by such monitoring.

6.3 Sometimes it is necessary for the Company to access your business communications during your absence, such as when you are away because you are ill or while you are on holiday. Unless your mailbox settings are such that the individuals who need to do this already have permission to view your in-box, access will be granted only with the permission of two of the persons authorised to grant such access, in accordance with clause 6.7.

6.4 Any emails that are not stored in your 'Personal' folder in your mailbox and which are not marked PERSONAL in the subject heading will be treated, for the purpose of availability for monitoring, as business communications, as we will have no way of knowing that they were intended to be personal. Therefore you must set up a rule to automate the routing of personal email to your personal folder – ask IT Support for guidance on how to do this. Furthermore, there is a risk that any person authorised to access your mailbox may have their own preview pane option as a default setting, which would reveal the content of any of your personal email not filed in your "Personal" folder, whether or not such emails are marked PERSONAL. It is up to you to prevent the inadvertent disclosure of the content of personal email by filing your personal email in accordance with this policy. In particular, you are responsible to anybody outside the Company who sends to you, or receives from you, a personal email, for the consequences of any breach of their privacy that may be caused by your failure to file your personal email.

6.5 In certain very limited circumstances we may, subject to compliance with any legal requirements, access email marked PERSONAL. 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.

6.6 All incoming emails are scanned by the IT department on behalf of the Company, using virus-checking software. The software will also block unsolicited marketing email (spam) and email which have potentially inappropriate or harmful attachments. If there is a suspected virus in an email that has been sent to you, the sender will automatically be notified and you will receive notice that the email is not going to be delivered to you because it may contain a virus.

6.7 Access, viewing or monitoring of an individual's accounts, including but not limited to emails and files, requires express written approval from two of the following – Group Managing Director, Human Resources Director.

6.8 Persons should be aware that they may not be notified if access has or is being granted to their accounts and/or files, in line with the aforementioned clauses.

7. Data Protection

7.1 As a member of the Company who uses our communications facilities, you may be involved in processing personal data for the Company as part of your job. Data protection is

about the privacy of individuals, and is governed by the General Data Protection Regulation (GDPR) and the Data Protection Act 1998 & 2018. Whenever and wherever you are processing personal data for the Company, you must keep them secret, confidential and secure, and you must take particular care not to disclose them to any other person (whether inside or outside the Company) unless authorised to do so. Further information on our rules and requirements for data protection is given in the Data Protection Policy.

8. Compliance with this Policy

Failure to comply with this policy may result in disciplinary action being taken against you under the Company's disciplinary procedures, which may include summary dismissal, and/or in the withdrawal of permission to use the firm's equipment for personal purposes. If there is anything in this policy that you do not understand, please discuss it with your line manager.

Please note that the procedures and policies outlined in this policy document, and in any related policy, may be reviewed or changed at any time. You will be alerted to important changes, and updates will be made available.

Policy edition: February 2007 // Revised May 2012 // Revised August 2016 // Revised March 2018 // Revised September 2021

Declaration

I have read the Company's Internet Acceptable Use Policy.

I acknowledge that the equipment with which I have been provided (and any software included) has been made available to me by the Company solely to assist me in the performance of my duties within the Company. It remains the property of the Company at all times.

I accept personal responsibility at all times for this equipment and any software included. In doing so, I agree to take all reasonable measures to protect this equipment and software from unauthorised use; to keep it in proper working order; and to follow the requirements of the Information Security Policy, Data Protection Policy and Social Media Policy where applicable.

I accept that the firm has a right to monitor my e-mail or Internet use as set out in this policy

I accept and understand that this declaration and the *Internet Acceptable Use Policy* form part of my terms and conditions of employment and hereby agree to abide by the terms laid out therein.

Name:

Signed:

Date: