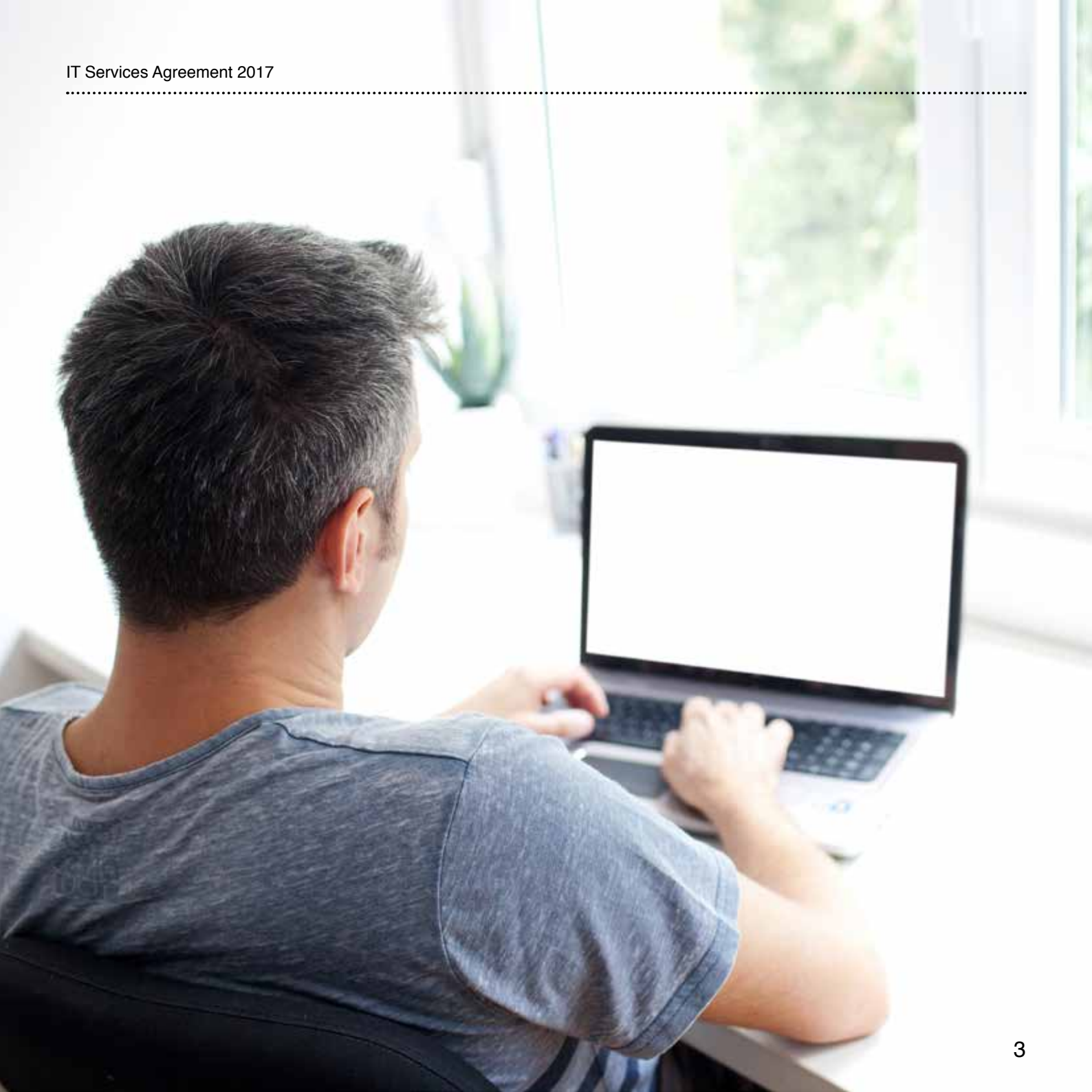
Acceptable Use of IT Policy 2017

SOUTH KESTEVEN DISTRICT COUNCIL

Contents



1. Purpose

This document details the policy for the acceptable use of IT assets and facilities at South Kesteven District Council (SKDC). This policy supports the continued successful operation of the Council such that the confidentiality, integrity and availability of its IT systems and data are maintained at a high level in keeping with the SKDC IT Services Agreement. There is also an obligation on the Users (see Scope below) to comply with relevant legislation such as the Data Protection Act, the Copyright, Designs & Patents Act, the Freedom of Information Act and the Computer Misuse Act.

The Policy is a framework by which SKDC lays down its expectations regarding the usage of its IT whether directly connected to the Councils infrastructure or used remotely.

Contained within this policy are the rules and parameters governing the secure and proper use of e-mail, the Internet, and Social Media. The policy has been devised in order to enable both the Council and its Users to gain the maximum benefit from its IT solutions, and aims to:

1. Protect the Council from potential legal liabilities;
2. Ensure the effective running of the organisation;
3. Prevent disruption caused by computer viruses;
4. Safeguard confidential and sensitive information;
5. Increase Users awareness of the legal, security and productivity issues relating to the use of e-mail and the internet;
6. Inform Users how they may and may not use computer facilities;
7. Encourage best practice.

2. Scope

This policy applies to all elected members (Councillors) and employees (officers) including temporary and contract workers, consultants, and those engaged through an employment agency who have been issued IT Assets by SKDC. This group is collectively referred to as the “Users” throughout this policy.

It also applies to Users who have access to the Council’s computer systems from home or whilst travelling. You should be aware at the outset that any breach of this policy may be regarded as a breach of our code of conduct and for employees, misconduct, leading to possible disciplinary action.

3. General Security and Confidentiality

3.1 GENERAL SECURITY

As a User you may be issued with a “standard build” computer that is best suited to your role within the organisation when you join. At this point you are responsible for the computer and any other IT assets you may be given, in terms of their operation and security, and any activities performed on them.

You must not in any way modify any computer system, software or computer installation without the guidance and permission of IT Services. This includes the installation of software. The IT Helpdesk is the preferred channel for raising any issues you may have which ensures that your issue is tracked properly and that IT Services can communicate with you effectively. Details about the IT Helpdesk can be found on the Homepage of our Intranet (Monty).

You should not leave your computer logged on and unattended. When leaving the computer for a period of time, you should “lock” it. This can be done by pressing the Win+L.(Windows and “L”) keys on your keyboard.

To support the above, computers provided by SKDC will automatically lock if left inactive or unattended for 5 minutes.

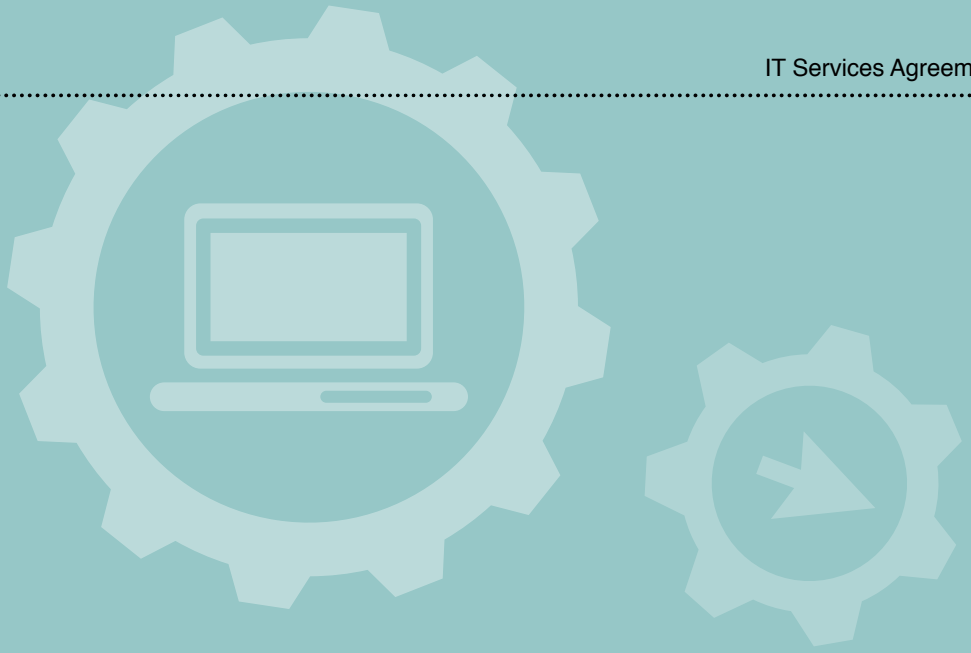
All passwords must be kept confidential at all times and should not be disclosed to anyone else. Your Line Manager or Political Group Leader should be notified immediately if there is a suspicion that another User is using a colleagues password.

Passwords must follow best practice and conform to the standards described in the IT Security Policy. For computers provided by SKDC, this policy is enforced automatically, so you will be asked to renew your passwords every 90 days when you log in.

3.2 REMOVABLE DEVICES

Files or other material must not be loaded from a CD, USB key or any exchangeable media that has been brought into the Council from an external source unless the media has been virus checked by the IT Services department.


Username
user
Password
****
Login



Files or other material must not be loaded onto a CD, USB key or any exchangeable media unless they are encrypted. Our standard builds provide encryption tools from McAffee that do this automatically for you.

3.3 USING PERSONAL IT ASSETS (MEMBERS ONLY)

Elected Members are permitted to use one piece of their own IT equipment. This is purely for the purposes of accessing Council e-mail and must be used in accordance with this Acceptable Use Policy. To meet our Code of Connection these devices must utilise the Airwatch Platform which must be installed by IT Services.

3.4 SOFTWARE

In order to minimise the risk of viruses entering the Council's computer network and to comply with licensing agreements, you are expressly forbidden to download software from the Internet or to load unauthorised software on to any PC or server from any media.
IT staff regularly audit our PCs and other IT assets. Any contraventions to this rule will result in the immediate removal of the software, and may lead to disciplinary action where appropriate.

3.5 VIRUS WARNINGS

If a virus warning appears on your computer screen at any time, you must immediately notify IT services on 6270 and shut the computer down until an IT support officer visits.


#cybercrime

4. E-mail/Texting/ Handling Documents

4.1 UNDERSTANDING CONFIDENTIALITY

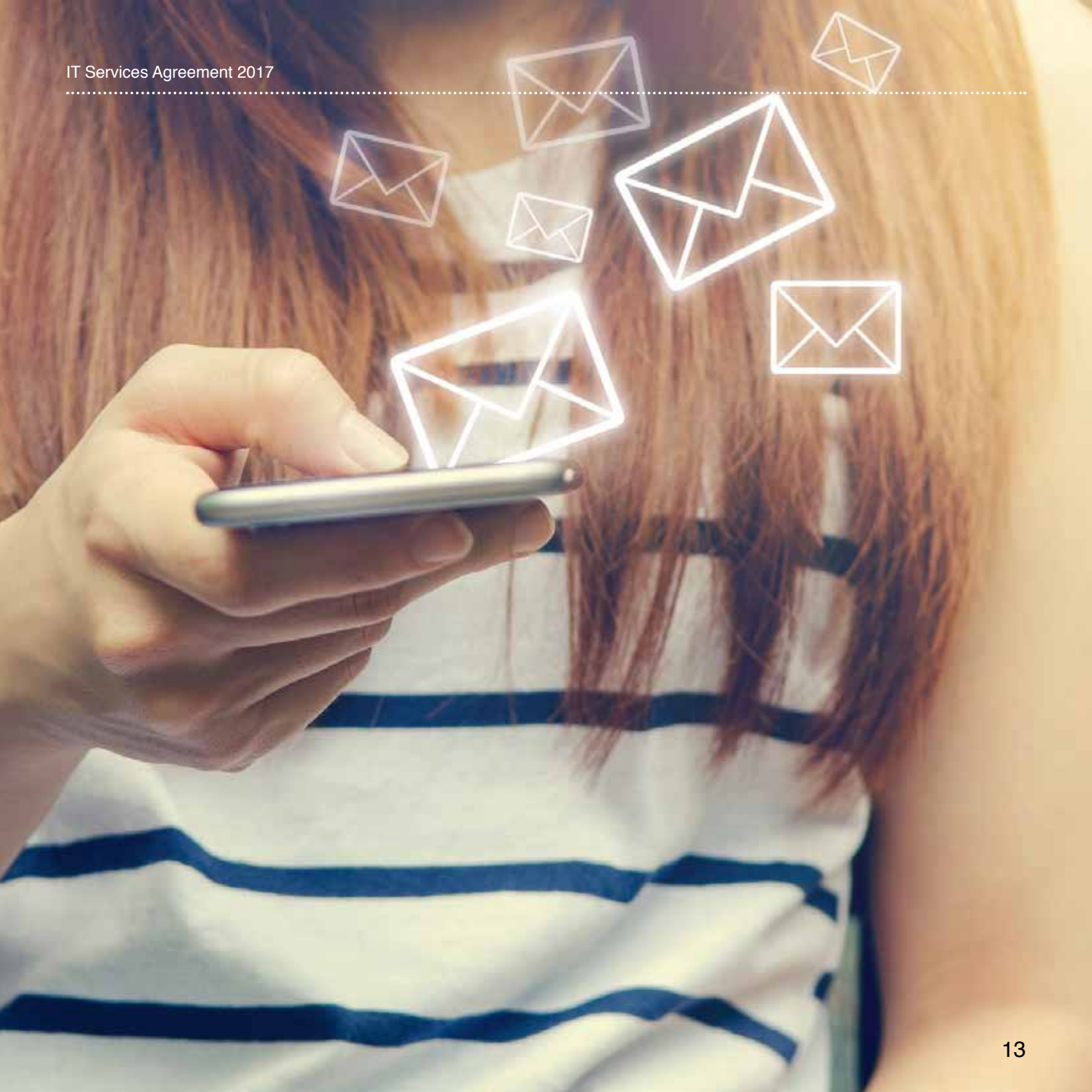
The sending of e-mail, messages and texts on either your computer or mobile phone should not be regarded as a secure or guaranteed method of communication. You also need to be aware that once you have sent something it is very difficult, if not impossible to retract it.

For those working with personal data (as defined by the Data Protection Act) or accessing data through the Government Gateway (eGov) as part of their role, confidentiality takes on a more formal context in how we have to handle the material. The Legal team have published advice on Monty regarding personal data and the Data Protection Act and its requirements. The following section discusses the use of official documents where protective marking may also be found.

4.2 PROTECTIVE MARKING

The protective marking of documents including e-mail is not used currently at SKDC. However, you may encounter this if you are working with documents issued by other Government Departments and Agencies.

The UK policy for the Protective Marking of documents (or their Security Classification) comes under the scope of the Cabinet Office. The marking scheme was relaxed and simplified following the issue of the latest policy in April 2014. So it is now highly unlikely that anything other than “Official” level documents will be encountered.
A copy of the Policy is available on the IT Services Page on Monty. It discusses how the different levels and types i.e. “Official – Sensitive” are derived and how documents are to be treated in use.



4.3 USING E-MAIL

The Council provides its Users with access to an e-mail Account for work-related purposes. Personal use of the council's e-mail system is limited to use as a point of contact i.e. so that schools or a childminder can contact a parent. Under no circumstances should Users personal e-mail accounts be used for council related business. In particular SKDC e-mail addresses should never be used to register with online websites for instance services such as online shopping, non-work related forums, Facebook, Myspace, EBay, Social Media not listed here etc.

4.4 ATTACHMENTS TO E-MAIL

The use of e-mail attachments is one of the favoured routes for "attackers" to try and introduce viruses and other forms of malware onto our systems. To make things worse it is a constantly changing threat to us. Be vigilant and use due diligence. Think twice before opening attachments. So for example it is very unlikely that your bank or HMRC would contact you by e-mail and ask you to click on a link or attachment to provide your personal details.

Don't open and please report suspicious e-mail to IT Services via the Helpdesk and they'll check it for you. To help, we have published more guidance on Monty and this includes a link to an excellent site provided by the "getsafe.org" government body. This talks about the different threats and provides advice useful in both your professional and personal lives.

5. The Internet

Users should bear in mind that because the Internet is largely unregulated, information from it may not necessarily be accurate, up-to-date or reliable.
Users are granted access to the Internet for the following purposes: -

- To seek information on matters that are relevant to your work/ function;
- To carry out on-line transactions relevant to your work/ function;
- For the purpose of work-related education/research,

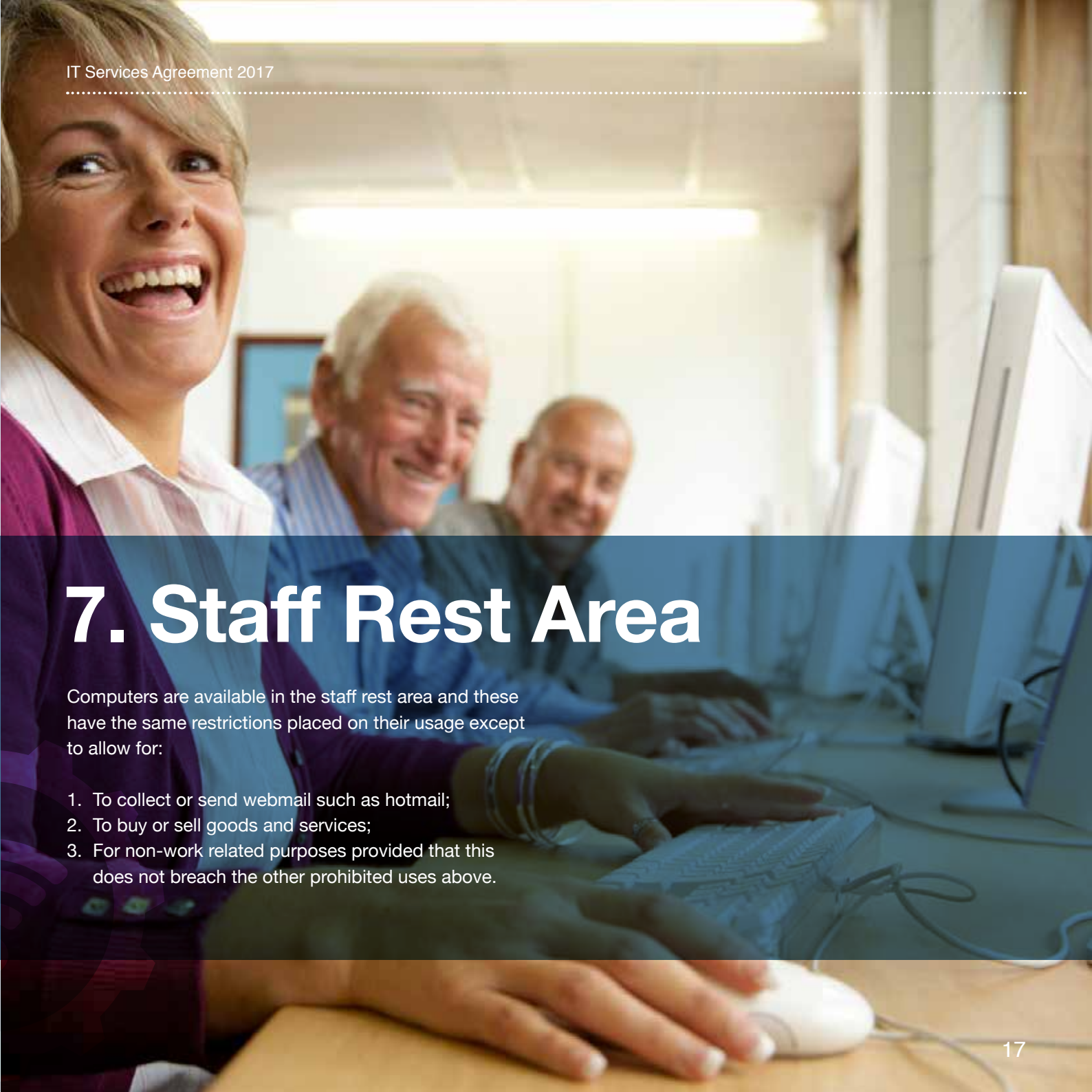
Limited personal use of the Internet is permitted provided that this does not interfere with your work and is kept to a minimum.

The law of copyright applies to electronic communication in the same way as it does to printed material and other forms of communication. Information posted on the Internet, although available to the general public, may be subject to copyright restrictions. Users should therefore be cautious when downloading and distributing documents from the Internet.

6. Prohibited Uses

This section is written on the basis that you should assume anything you put out on the internet, or social media by e-mail, text or messaging cannot be retracted. You may not at any time use your SKDC IT Assets for any of the following purposes: -

- To transmit text or other material that may be regarded as sexually explicit or in contravention of the Council's equal opportunities or generic equality policies;
- To communicate anything that is illegal, or that could be interpreted as defamatory, derogatory, intimidatory, rude or offensive, whether internally or externally;
- To compile, send or forward chain, joke or junk messages whether internally or externally;
- To send or forward e-mails as though from another person unless your Line Manager or Political Group Leader has, in writing, expressly requested you to send e-mails on their behalf and in their name;
- To use for political purposes other than those pertinent to the management of the Council and for the Members in the discharge of their duties.
- SKDC IT Assets for electoral purposes i.e. canvassing
- To create or transmit defamatory material;
- To disseminate material that may bring SKDCs name or the name of any of its officers or members into disrepute or that would cause embarrassment to SKDC;
- To access or download knowingly indecent or improper, or any type of offensive or illegal material;
- To download, copy or distribute software, graphics, or screen-savers;
- To carry out any freelance work unrelated to SKDCs business, to gamble, contribute to Internet newsgroups, play games or participate in issues not related to SKDCs business;
- To breach copyright;
- To breach the IT Security Policy and/or any other SKDC related policy.



7. Staff Rest Area

Computers are available in the staff rest area and these have the same restrictions placed on their usage except to allow for:

1. To collect or send webmail such as hotmail;
2. To buy or sell goods and services;
3. For non-work related purposes provided that this does not breach the other prohibited uses above.

8. Monitoring

Monitoring is used for a number of purposes primarily for legal reasons or for the protection of our Users and IT Assets. It is not there to spy on people or to have a "back door" into our data to try and catch people out.

The monitoring covers the use of our e-mail system and Internet access amongst other things. Software is also in place to prevent access to sites containing offensive, illegal or unsuitable material.

The specific reasons for monitoring are as follows: -

- To protect the Council against legal liabilities;
- To uphold the Council's e-mail and internet policy and safeguard against misuse of these communication systems;
- To check e-mails and e-mail attachments for viruses and offensive material for the protection of all staff;
- To guard against excessive personal use of the Council's communications systems;
- To provide a record of transactions that may form part of contractual agreements;
- To provide audit trails of license usage;
- To guard against computer viruses.

8.1 MONITORING OF INTERNET USAGE

Users who have Internet access during the course of their work should be aware that SKDC may track the history of the Internet sites they have visited.
SKDC will treat the results of monitoring in strictest confidence and in accordance with the requirements of the Data Protection Act.

8.2 E-MAIL LOGGING AND ARCHIVING

Users need to be aware that e-mails stored are the property of SKDC and that logging and archiving systems are used. The primary purpose of this is to protect the security of the Council's business. With the permission of the relevant Line Manager or Political Group Leader, Legal and Democratic Services and the IT Business Manager, individual e-mails can be remotely examined where there is a clear justification and in keeping with the UK Data Protection Act.

SKDC has introduced an e-mail archiving solution, which will retain all e-mail and attachments sent and received in accordance with SKDC and legal defined retention guidelines. Archived e-mail is protected from being edited and is searchable for Freedom of Information and Data Protection purposes.

9. Breaches

Any person who is found to have breached this policy may be subject to disciplinary action.

9.1 REPORTS OF BREACHES

If you are concerned that a colleague is abusing SKDC's IT Policies or acting in any way contrary to this policy, you are encouraged to disclose the abuse in confidence to your Line Manager or Political Group Leader.
Any complaint of e-mail or Internet abuse will be treated seriously, confidentially and promptly investigated.