Acceptable Use Policy

2023

SOUTH KESTEVEN DISTRICT COUNCIL

Purpose and applicability

This policy defines the acceptable use of South Kesteven District Councils (SKDC) information assets and those assets provided to the council by partner organisations. It is known as the **‘Acceptable Use Policy’ or ‘AUP’.**

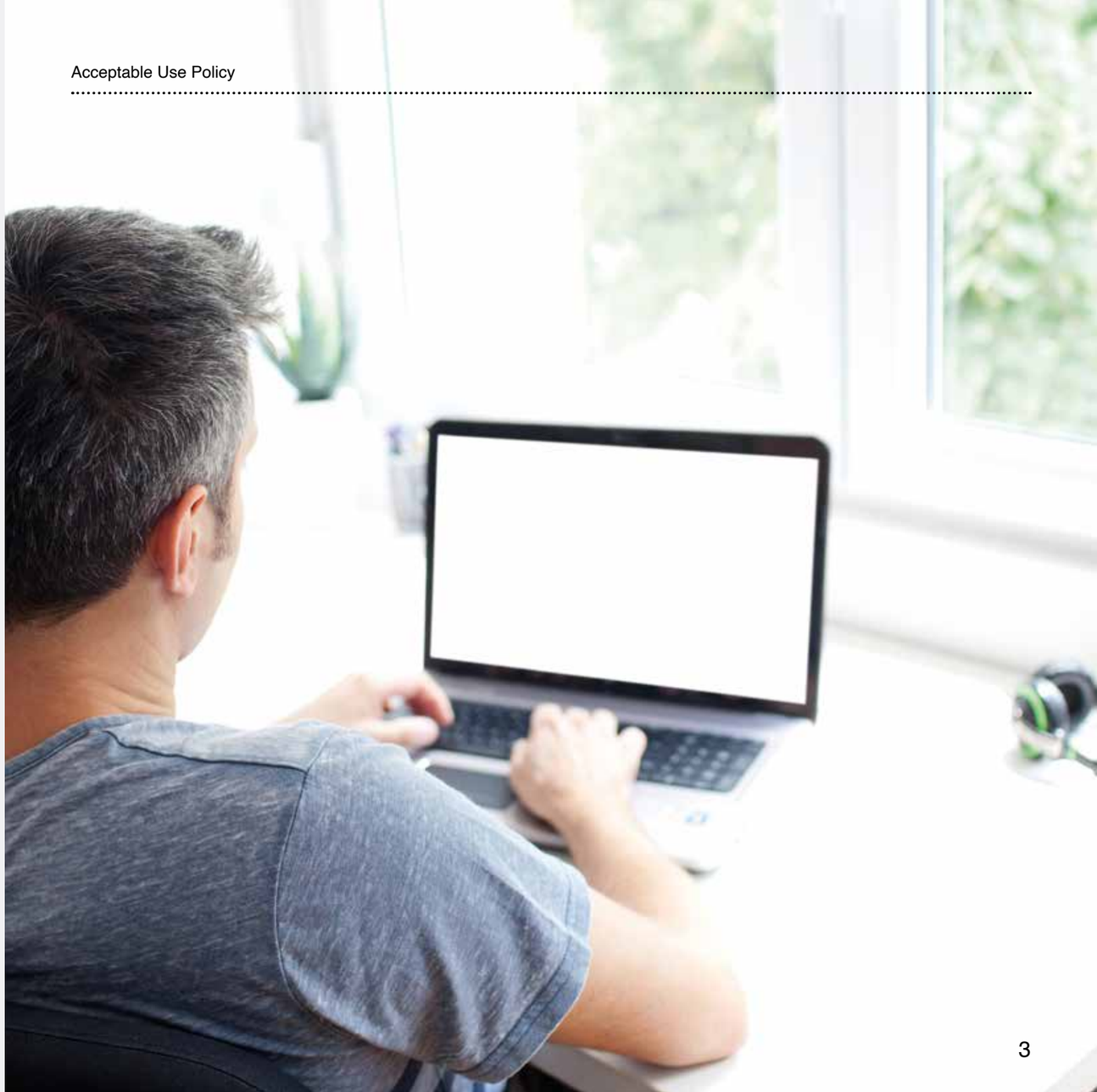
This policy applies to council workforce including temporary and agency workers, volunteers, independent consultants and suppliers/contractors who need to use council information assets, as part of/to carry out their duties. These people are referred to as ‘users’ in the rest of this document.

Acceptable use means that access to information is legitimate, it is used only for the intended purpose(s), the required standards of practice are in place to protect the confidentiality, integrity and availability of information, and the use complies with relevant legislation and regulation.

The council aims at all times to conduct its business in a professional manner and to provide the highest possible level of service, both internally and to its customers.

Any loss, compromise, or misuse of council information and associated assets, however caused, could have potentially devastating consequences for the council and may result in financial loss and legal action.

Acceptable Use Policy



Definitions

An **information asset** is any data, device, or other component of the environment that supports information-related activities. Assets include hardware (for example, laptops, and handheld phones), software and confidential information (for example, a person's record).

Inappropriate use of information assets exposes the council and the service users who entrust us with their data to risks.

A **data subject** is a person or organisation to whom data relates.

A **data controller** is a person or organisation who is legally in charge of a data asset. The council is the data controller for many of the assets it holds.

A **data processor** is a person or organisation who is tasked by a data controller with using a data asset. The council is a data processor for some organisations such as the NHS and Police.

A **user** is any person or organisation accessing information assets.

Personal data is data that relate to an individual. For example, your name, address and date of birth are examples of your personal data. **Special Category personal data** is data revealing 'racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'. This is commonly referred to, along with other data, such as financial information, as 'sensitive'.

'PC' means any computer device such as a tablet, laptop or desktop computer.

'Handheld' means any portable device with a mobile network connecting including smart phones, mobile phones, Andriod Tablets or iPads.

Policy statements

It is the responsibility of all users to know this policy and to conduct their activities accordingly. Breach by any user could result in disciplinary action or other appropriate action being taken.

Council information facilities are provided for business purposes only, with limited personal use permitted as defined elsewhere in this document.

Use of information facilities must be authorised by line managers.

Any use of council facilities for unauthorised purposes may be regarded as improper use of facilities.

Users should be aware that any data they create on council systems (including anything pertaining to themselves) is deemed to be the property of SKDC. Users are responsible for exercising good judgment regarding the reasonableness of personal use and to be compliant with the Employee Code of Conduct.

For security and network maintenance purposes, authorised users may monitor equipment, systems and network traffic at any time. The council reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

The policy is not designed to be obstructive. If you believe that any element of this policy hinders or prevents you from carrying out your duties, please contact IT Support.

Use of personal data

The council has access to a wide range of personal data entrusted to us by our citizens and others. This data must be used and accessed in accordance with the law.

Users must only use personal data in accordance with the agreed and published purposes for the collection of data. Using personal data in any manner requires a clear legal basis or consent from the data subject. Merging personal data with other sources, for example, is not permitted unless a legal basis or consent is present, and the use of the data is correctly authorised.

Information system security

Security controls and reporting

The council has implemented security systems to safeguard information assets. These include controls over viruses, offensive and illegal material, disruption to our systems, and unauthorised access. Bypassing or attempting to bypass these security systems is a breach of policy.

To be effective, all users must support and use these systems and must assist in identifying and eliminating threats to information security. Any breach or suspected breach of this policy must be regarded as a security incident.

Users must report security incidents to IT Support immediately.

Use of downloaded programs

Under no circumstances may users use any program that is not already installed on a PC or download programs from the Internet for use on council systems. For handheld devices, only applications from approved app stores should be installed.

If you do require any programs or apps not already installed or available you should contact the IT Support desk for assistance.

Passwords

Users are responsible for the security of their passwords and accounts. Passwords must be kept confidential and not shared with others.

Temporary passwords for new users must be changed at the first log-on.

Internet usage

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.

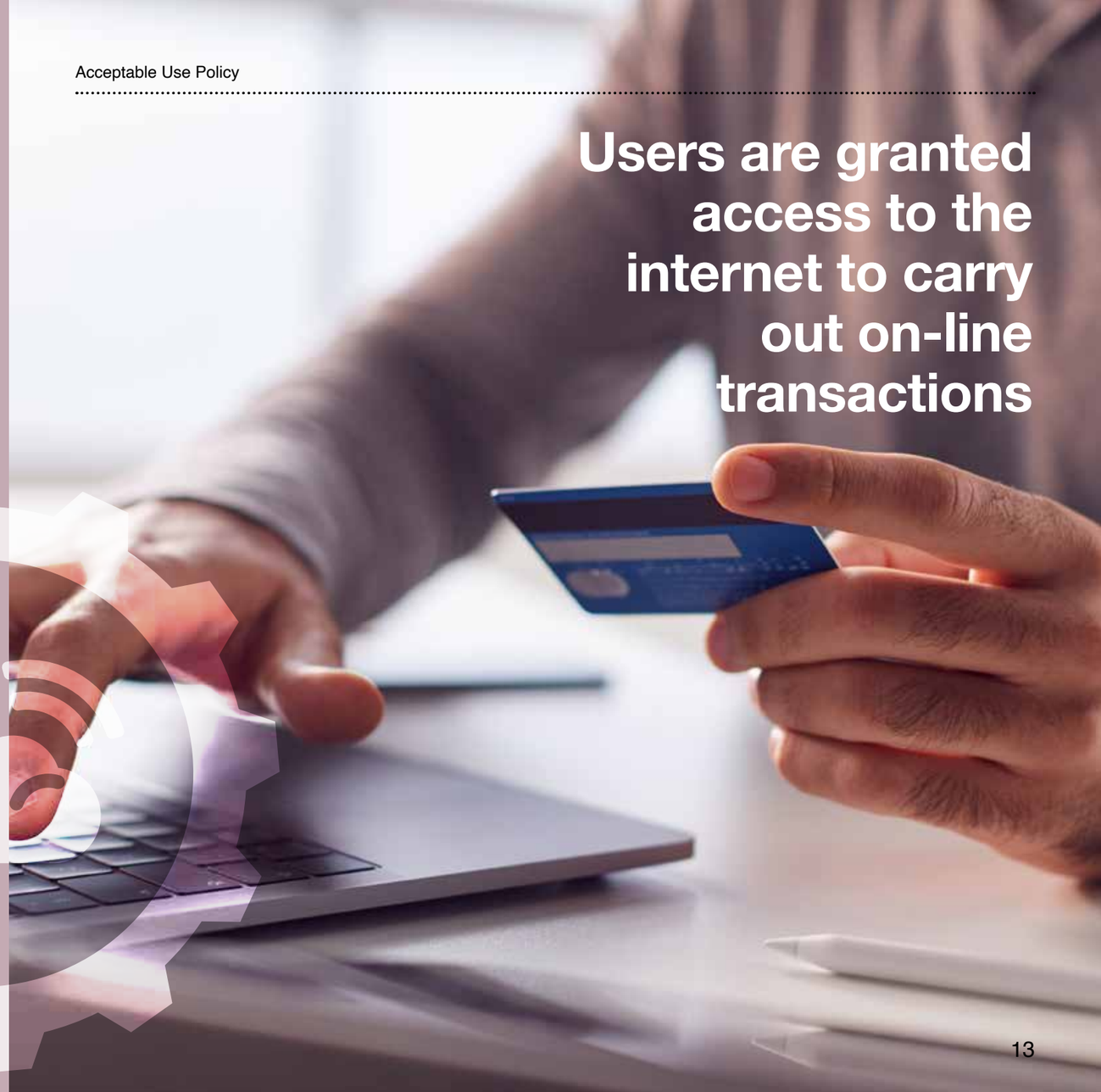
Users are granted access to the Internet for the following purposes: -

- 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, and pages visited are known sites.

The law of copyright applies to electronic communication in the same way as it does to printed material and other forms of communication. The 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.

Acceptable Use Policy



Users are granted access to the internet to carry out on-line transactions

Email usage

The email system is for council business use only. All communications from an SKDC email address should only relate to council information. Also, registration to any services using the SKDC email address as the username or contact must only be for work purposes. Access to webmail systems such as Gmail or Hotmail is available from Council devices for personal accounts but should be limited to breaks or outside of working hours unless permission is given by a line manager.

Auto forwarding of emails to external email accounts is expressly forbidden.

Emails that users intend to send should be checked carefully. Email should be treated like any other form of communication and, as such, what is normally regarded as unacceptable in, for example, a letter is equally unacceptable in an email communication. The sender of the email is responsible for the safe arrival of information at its intended destination and it is the sender who is usually liable for any breach of security and confidentiality.

Sending emails internally is secure. Sending emails externally is not generally secure and they can be intercepted and viewed by unauthorised people. Secure email must be used when emailing information to external agencies or individuals when the content of the email includes:

- Personally identifiable client or third party information.
- Financial, sensitive or other information that could cause detriment to the council or to an individual.

Personal or sensitive business information must not be sent to an email address outside of SKDC, unless it is absolutely necessary and the transmission is secure. This can be done using:

- Microsoft Office 365 mail to government agencies (.gov.uk, .nhs.net etc).
- Microsoft Office 365 encryption

Staff must be vigilant with attachments to emails and links to documents downloaded from other locations as they may contain viruses. Users who suspect a possible virus attack must report it to IT Support immediately. Staff must be aware that email is easy to forge and that attacks based on this are common. Always treat emails asking for unusual actions with suspicion.

For example:

- Any email asking to move money should be confirmed in person or by telephone.
- Any email asking for a password or to click on a link which then asks for username, password or bank details even if it appears to be from SKDC may be fake – SKDC will never ask for these details.
- Emails containing urgent invoices are likely to be fake – invoices should go via our scanning facility to be matched to the E-procurement system.

For further information regarding secure information exchange (for example, via email and Cloud Storage) please refer to the ‘Data Protection Policy’

Responding to security incidents and malfunctions

Any perceived or actual information security incident must be reported to IT Support immediately. Examples of a security incident include unauthorised access to information assets, misuse of information assets, loss/ theft of information assets, virus attacks, denial of service attacks, or other suspicious activity.

Computer viruses and other harmful code

All PCs and servers directly connected in the Council offices, are protected by virus scanning software, and the councils firewalls but you should still be careful and vigilant when using the internet and opening emails.

When you are working remotely, extra care should be taken. Email and internet controls are still in place but the network being connected to is out of SKDC control so should only be used if it is your home or another trusted source.

It is a crime under the Computer Misuse Act 1990 to deliberately introduce malicious programmes into the network or server (for example, viruses, worms, Trojan horses, email bombs). Users must not use council facilities for intentionally accessing or transmitting computer viruses or other damaging software or software designed for creating computer viruses.

If you are in doubt about any data received or suspect a virus has entered your PC, log out of the network immediately, stop using the PC and inform the IT Support. You should always follow the instructions that the service desk issues about virus attacks.

Never forward any emails you are suspicious of to another user unless specifically request to by IT Support.

Hacking and associated activities or breaches of policy

It is a crime under the Computer Misuse Act 1990 to enter into another computer system without authorisation.

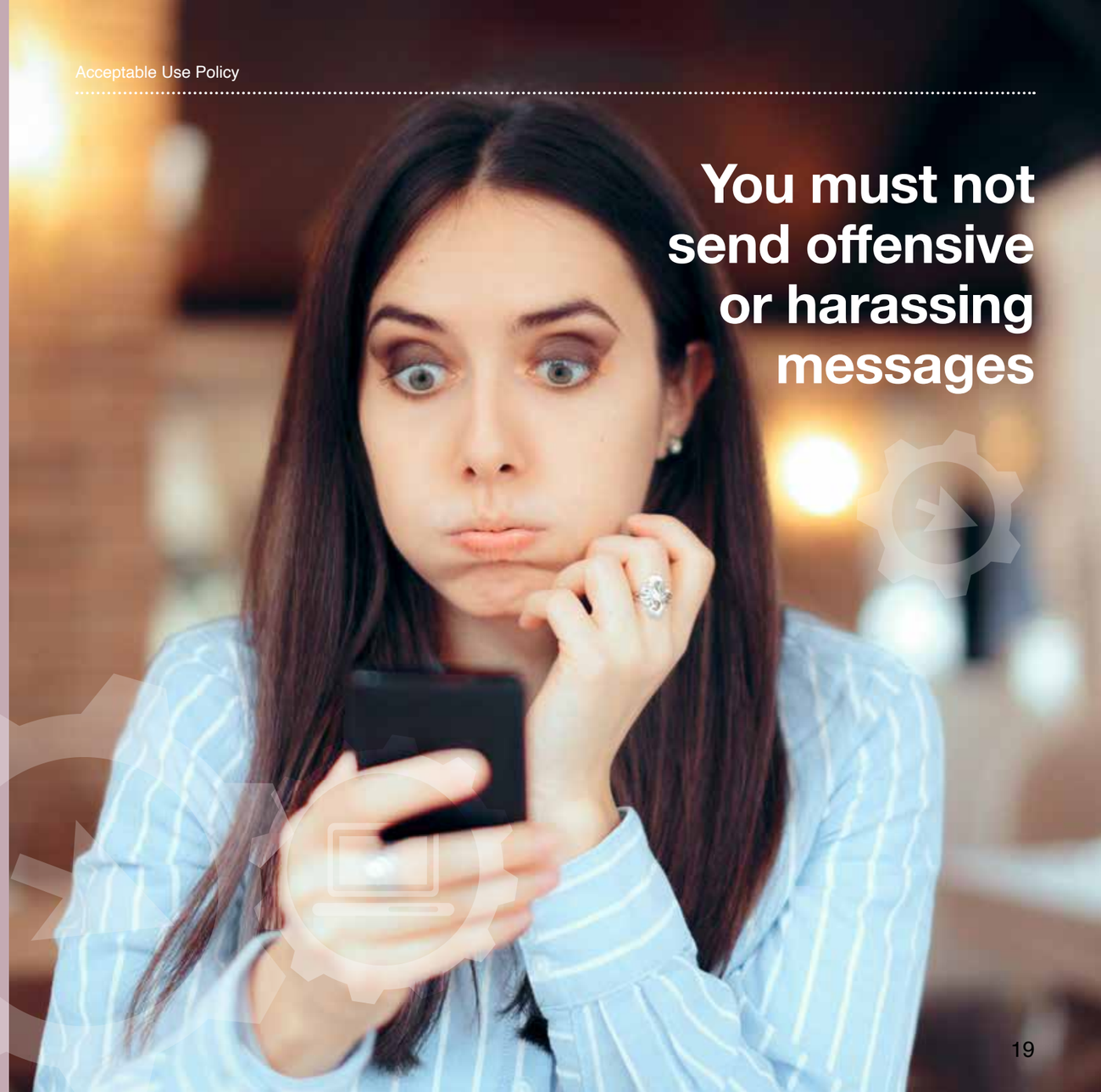
Council IT facilities must not be used in any way that breaks the law or breaches standards. Such actions could result in disciplinary action being taken.

Users must not use council facilities for:

- Sending threatening, offensive or harassing messages
- Creating or sending obscene material
- Accessing or transmitting information about, or software designed for, breaking through security controls on any system.
- Effecting security breaches or disruptions of network communication. These include, but are not limited to:
- Accessing data to which the user is not an intended recipient without permission, even if it is not protected by security controls.

- Logging into a server or account that the user is not expressly authorised to access
- Network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes
- Port scanning or security scanning (unless prior authorisation has been granted)
- Executing any form of network monitoring which will intercept data not intended for the user (unless prior authorisation has been granted)
- Circumventing user authentication or security of any host, network or account
- Interfering with or denying service to any user (for example, denial of service attack)
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's communication session, via any means, locally or via the Internet / Intranet / Extranet.

Users may be exempted from some of the above restrictions during the course of their legitimate job responsibilities (for example, systems administration employees may have a need to disable the network access of a host if that host is disrupting production services). Such exemptions should be reported to and approved and documented by the IT Manager.



Copyright and encryption

It is illegal to break copyright protection. Users could break copyright if they download, transmit or copy protected material.

Users must not:

- Transmit copyright software from their PC or allow any other person to access it from their PC unless the controls/licence so permits
- Knowingly download or transmit any protected information/material (including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources and copyrighted music) that was written by another person or organisation without getting permission
- Copy/install copyright software from/to their PC for any purpose not approved by the licence and for which SKDC or the user does not have an active licence
- Transmit software, technical information, encryption software or technology, in violation of international or regional export control laws.
- The IT Manager should be consulted prior to the export of any material that is in question and all information in this respect should be documented accordingly.

Unattended user equipment

Users must not leave their workstation unattended without locking the device first, this is especially important when working remotely.

Users accessing sensitive information must position their workstation in such a way that the information is not visible to unauthorised users.

No paper copies of data, memory sticks or other portable media may be left on desks when unattended.

Computer usage

All council owned computer equipment and software remain the property of the council. Any user who leaves council employment / engagement is required to return all hardware and software that has been provided to them.

Only hardware provided by the council is authorised for use for council business, except when a personal handheld device has been approved for use by the IT department and correctly registered for access.

Software usage

SKDC is committed to the use of only authorised and licensed software within its computer systems. It is expressly forbidden for users to load or operate software gained from the Internet, or other sources unless agreed and approved by the IT department.

It is the responsibility of all users to ensure that they do not introduce viruses into computer systems. Users should take care when receiving electronic information from unknown sources, including attachments within email. Where there are reasons to access information from questionable source(s), active virus checking must be performed, preferably on a standalone computer and/or test server, thus having no communication links to other systems.

The following provisions, which apply to the use of all computers, govern all users:

- Only software purchased by SKDC and approved by IT may reside on SKDC computer equipment including PCs and handhelds.
- IT will undertake to purchase licences for all products used by SKDC and will control the allocation of licences for products that are distributed as single media items and licences for multiple instances of that one distribution.
- Only IT authorised technical staff may install or remove software on SKDC computer equipment.
- Software includes source code, object code and intermediate code that can be firmware as well as software.
- Downloading of ‘shareware’ and/or ‘freeware’ is prohibited irrespective of the fact that a licence may or may not be needed unless IT has approved the product to be downloaded and installed.
- The installation of personal software even if licensed is prohibited
- Upgrades to software products should also be approved by IT as they could affect the license validity

Handheld devices

Devices such as smartphones and tablets provided by the Council are protected by central management controls. It is the user’s responsibility to ensure the device software and apps are kept up to date. Failure to do so could lead to the device becoming non-compliant and losing access to council systems.

To ensure that a handheld cannot be used fraudulently, IT policy requires that devices are secured by a PIN number or biometric controls. If a council mobile phone is lost or stolen it must be reported to IT Support.

For mobile phones, voicemail should be checked regularly and greetings updated as necessary if used. If a device is lost or stolen, IT Support must be contacted as soon as possible.

Access from overseas

The user should seek advice from IT Support before taking any council supplied IT equipment outside the United Kingdom. Handheld devices with data contracts are not covered in all countries so advice can be given before traveling.

Landline Telephones

Personal calls should be kept to a minimum and not interfere with performance of duties. The council reserves the right to check, review and monitor telephone calls made using any council telephone or telephone system.

Where the council provides a user with a mobile phone, it is to ensure that the user is contactable when away from the office. Therefore, council mobile phones should be switched on or directed to voicemail or an alternative phone at all times during working hours.

Voicemail should be checked regularly and greetings updated as necessary. Voicemail users should secure their messages with a minimum four-digit pin code and clear down messages on a frequent basis.

Legislative requirements

Under no circumstances are users allowed to engage in any activity that is illegal under local, national or international law while utilising council resources.

Monitoring use

The council reserves the right to monitor, review and record the use of all information and telephone systems and all documents stored on information systems, including documents profiled as private and confidential.

The council reserves the right to monitor email traffic within the corporate email system and to access mailboxes and private directories without notification to the individual concerned that the right is being exercised.
The council may exercise this right in order to establish facts relevant to council business and to comply with:

- Regulatory practices and procedures
- To prevent or detect crime
- To ensure compliance with council policies
- To investigate or detect unauthorised uses of the system or to ensure the effective operation of the system (for example, to check if viruses are being transmitted)

Therefore, users do not have the right to privacy when using council information systems or in relation to any communications generated, received or stored on council information systems.

Policy compliance

The council expects that all users will achieve compliance with the directives presented within this policy. This policy will be monitored by the Corporate Information Governance Group, and compliance checks will take place to review the effectiveness of its implementation.

Exceptions

In the following exceptional cases compliance with some parts of the policy may be relaxed. The parts that may be relaxed will depend on the particular circumstances of the incident in question.

- If complying with the policy would lead to physical harm or injury to any person
- If complying with the policy would cause significant damage to the company's reputation or ability to operate
- If an emergency arises

In such cases, the user concerned must take the following action:

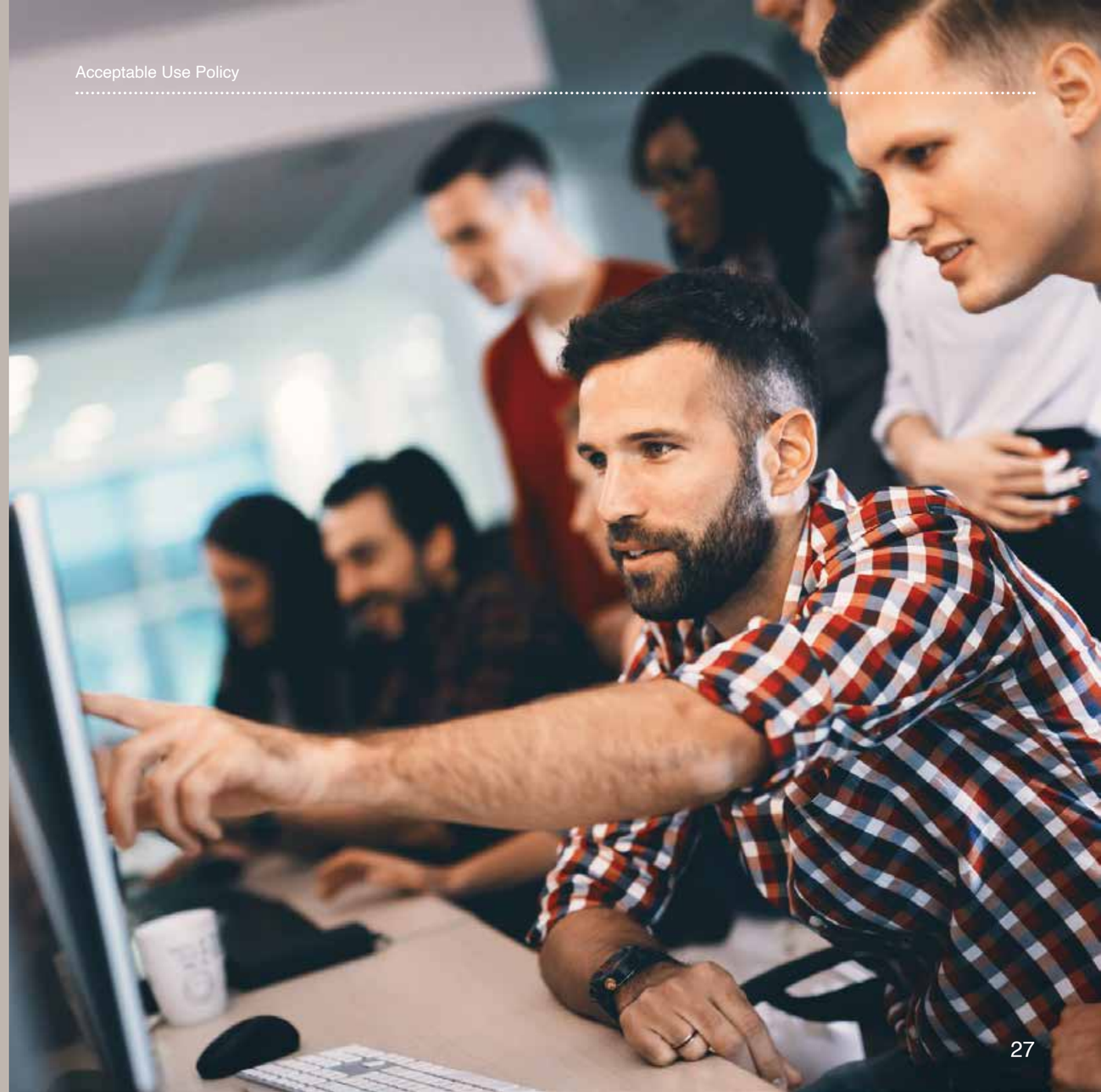
- Ensure that their manager is aware of the situation and the action to be taken
- Ensure that the situation and the actions taken are recorded in as much detail as possible on a non-conformance report
- Ensure that the situation is reported to IT Support (who will inform the IT Manager) as soon as possible.

Failure to take these steps may result in disciplinary action.

In addition, the IT Manager maintains a list of known exceptions and non-conformities to the policy. This list contains:

- Known breaches that are in the process of being rectified
- Minor breaches that are not considered to be worth rectifying
- Any situations to which the policy is not considered applicable.

The council will not take disciplinary action in relation to known, authorised exceptions to the information security management system.



Penalties

Non-compliance is defined as any one or more of the following:

- Any breach of policy statements or controls listed in this policy
- Unauthorised disclosure or viewing of confidential data or information belonging to the council or partner organisation
- Unauthorised changes to information, software or operating systems
- The use of hardware, software, communication networks and equipment, data or information for illicit purposes which may include violations of any law, regulation or reporting requirements of any law enforcement agency or government body
- The exposure of the council or partner organisation to actual or potential monetary loss through any compromise of security
- Any person who knows of or suspects a breach of this policy must report the facts immediately to IT Support or senior management.

Any violation or non-compliance with this policy may be treated as serious misconduct.

Penalties may include termination of employment or contractual arrangements, civil or criminal prosecution.

Contact Details

Alternative formats are available on request: audio, large print and Braille

South Kesteven District Council
01476 40 60 80
customerservices@southkesteven.gov.uk
www.southkesteven.gov.uk

03734RT_3.23