Acceptable use of information and ICT Policy

Title	Acceptable use of information and ICT Policy
Document version	1.0
Release date	1/5/2018
Author	Tony Smith
Location of published policy	aspire intranet
Consultation	• Cabinet member for governance • Corporate Management Team • Legal • Policy • Trade Unions • Arvato
Approved by	
Equality Impact Assessment	Please refer to the Information Assurance Equality Impact Assessment.
Review date	1 year from publication

Contents

1. Policy statement

It is council policy that all personnel will take responsibility for managing information in accordance with this Acceptable use of information and ICT Policy.

This policy outlines how Chesterfield Borough Council (referred to as "the council" in this document) will protect its information assets and supporting assets by highlighting to users the policies, guidelines, and key messages that directly apply to them in their day to day handling of information and use of information systems to ensure its information is secure, allowing the information to be used effectively for delivering its services.

2. Scope

All personnel, physical locations, information assets, supporting assets and third parties as required.

3. Objectives

The main objectives of this policy are:

1. To ensure everyone handles council information or uses the council's information systems in accordance with the council's information assurance policies and guidelines
2. To manage risks to protect the confidentiality, integrity and availability of the information assets of the council affording additional protection to sensitive information
3. To comply with relevant legislation
4. To comply with contractual security requirements
5. To follow (where appropriate) information security best practices

6. To provide accountability to those people who protect the Council's information assets and supporting assets

7. To support efficient working practices

4. Roles & responsibilities

All personnel have a duty to ensure the council's information assets and information systems are used securely and efficiently.

5. Instructions

5.1. Supporting policies & guidance

5.1.1. Users are reminded that information and information systems must be used in accordance with the following supporting policies and guidelines

- Data Protection policy
- Information Security policy
- Information Security guidance

5.2. Key messages are also provided below to form a simplified code of conduct for users

Monitoring user's use of information systems

In order to enforce its policies the council monitors the use of its information systems in accordance with the law.

Disciplinary procedures for misuse of council information and information systems

Personnel will be investigated in accordance with the council's disciplinary procedures. Any misuse by agency staff, contractors, or sub-contractors will be referred to their employers.

Human rights

The Human Rights Act 1998 gives certain rights to privacy for personal electronic communications in the workplace. The council reserves the right for authorised officers, in an act of investigating potential misuse or in supporting the council's systems, to access such communications.

Electronic documents may be inspected and copied as part of legal proceedings involving the council, under court procedures now known as 'disclosure'.

Computer misuse

The Computer Misuse Act 1990 covers unauthorised or malicious use of any computer system. It is used to prosecute hackers and people who write and distribute computer viruses deliberately.

It is a criminal offence to access, or attempt to access, any computer system you are not authorised to access. This law protects against employees and members of the public who deliberately cause damage to systems or data. The Act also makes it illegal for a person to deliberately delete data or sabotage systems to the detriment of the council.

Harassment

It is possible to commit harassment by using e-mail to send a harassing message to someone or by downloading and distributing material from the internet that creates an intimidatory working environment. Harassment and discrimination are unlawful under the Equality Act 2010 and Protection from Harassment Act 1997.

As with any form of harassment under the anti-discrimination legislation, the intention of the parties is irrelevant. Every individual in the organisation has a duty to promote a non-intimidatory working environment.

Obscene Material

Publishing legally 'obscene' material is a criminal offence under the Obscene Publications Act 1959. This includes electronic storing and/or transmitting of obscene materials that would tend to deprave and corrupt or any paedophiliac material. Any instances of this nature found will be reported directly to the Police.

Defamation or false statements

Liability for defamation or false statements applies to electronic communication just as it does to more traditional forms of communication. Anyone who e-mails a libellous or false e-mail message or posts such a message on the internet will be responsible for it and liable for any damage it causes to the reputation of the victim.

In addition to the liability of the individual who made the libellous or false statement, the council may also be held liable. This could be either under the normal principles of:

- indirect liability because the council is considered responsible – known as 'vicarious liability'

or

- direct liability as a publisher because of providing the link to the internet or e-mail system

An untrue statement that damages the reputation of a person or company by causing people to think worse of them will generally be defamatory. Similarly, a false statement intended to cause damage to a person or their economic interests can bring a claim for damages.

Reporting ICT related faults to the ICT Service Desk

Employees reporting ICT related faults should contact the ICT Service Desk by phone ext. 5253 or by e-mail to the ICT Service Desk.

The fault report will be noted and logged onto the ICT Service Desk system. An ICT Support Officer, allocated to resolve the fault report, will contact you to discuss/remedy the fault as soon as possible.

Incident response for lost, stolen or misplaced end user devices

Users must report lost, stolen or misplaced end user devices to their line manager and to the ICT Service Desk.

Using removable media

The use of removable media is restricted.

Users must request the use of removable media via the ICT Service Desk.

Training

Users should ensure they have received suitable training before accessing information and information systems.

Hardware and Software Acquisition

Requests to purchase any hardware and software must be in accordance with the council's procurement and project management procedures. This includes all computer hardware, software or services. All ICT related purchases must be made via the ICT service.

Software licensing & copyright

Managers should ensure that appropriate licences are purchased for any software in use by their staff.

Copyright laws may apply differently for each piece of software. In general, the copyright to every piece of software run on a system is owned by whichever company or person wrote it. The council has a legal duty to make sure sufficient licenses of the correct type are present to cover the use of all software.

No software can be loaded onto council systems without the organisation holding the appropriate licence to operate the software. Licences held by individuals that are not

held in the councils name will not suffice. All software licences should be purchased via the ICT service.

Reporting information security incidents

It is the duty of all personnel to report incidents to their manager, to the ICT Service Desk and to the Information Assurance Manager .

Sustainability

The use of resources such as paper should be reduced as much as possible. The following measures should be followed where printing is required:

- Always use duplex capable printers (printing on both sides of the paper) wherever possible
- Do not print paper copies of e-mail trails (only print required extracts)
- Read documents on an electronic device without printing
- Distribute documents electronically (preferably as a link to a centrally held copy)

Ensure that all non-shared ICT devices (i.e. computers and printers) are switched off when not in use. Where access is practical ensure that devices are switched off at the wall socket to ensure that ICT devices do not continue to use any standby power.

All ICT equipment must be returned to the ICT service for disposal in line with the European WEEE disposal (Waste Electrical and Electronic Equipment) directive.

All consumable items (such as ink cartridges and laser printer toners) issued by ICT services must be recycled.

In order to reduce both costs and the waste of consumables, the council has an active programme to reduce the number of printers, with a move to centralised, shared print facilities.

Confidential waste

Staff should utilise the confidential waste facilities provided or request confidential waste facilities from their line manager where they have not been.

Use of the “internet”

- Use of the internet for personal use is permitted provided the following applies:
    - It is in the employees own time
    - It is on a reasonable and occasional basis
    - It does not cause any disruption, disturbance, inconvenience or degradation of the service
    - It does not interfere with the work of the council

    - It does not interfere with other employees doing their jobs (in situations where computer are shared with other users)
    - council e-mail addresses (ending in .gov.uk) are not used for any registration when using the internet for personal use

- The council reserves the right to not provide services over the internet that have an adverse effect on productivity or are abused by individuals or groups of employees

- Use of the internet can have severe legal implications both for the employee and the council. Misuse can lead to disciplinary, criminal and civil proceedings. Disciplinary action may include action for gross misconduct

- Use of the internet for making financial transactions on behalf of the council will only be permitted, using systems implemented or authorised by senior management

- Any use of the internet to make payments for personal reasons is made entirely at the risk of the employee and the council accepts no liability

- If you require legitimate business access to a site that is blocked by the internet content filtering system you can contact the ICT Service Desk. They will then review the website, but they will only unblock the website if it is safe to do so

- If you knowingly enter a site that may be construed as unfit, obscene or inappropriate this could be considered as gross misconduct and be subject to a disciplinary investigation

- You should report any website that may cause offence (and is not blocked) to the ICT Service Desk so that they can block future access

Use of the e-mail system

- Use of the e-mail system for personal use is permitted provided the following applies:
    - It is in the employees own time
    - It is on a reasonable and occasional basis
    - It does not cause any disruption, disturbance, inconvenience or degradation of the service
    - It does not interfere with the work of the council
    - It does not interfere with other employees doing their jobs (in situations where computer are shared with other users)
- Use of e-mail can have severe legal implications both for the employee and the council. Misuse can lead to disciplinary, criminal and civil proceedings. Disciplinary action may include action for gross misconduct.
- 'All User' e-mails to employees and to council members is strictly limited
- Authorisation for sending e-mail communications to large groups of e-mail recipients should be requested from the council's Communications & Marketing Department to ensure the appropriate communication channels are being used
- You must not read, delete, copy or modify the contents of anyone else's mailboxes, unless this has been authorised by the appropriate level of management
- If you receive e-mail that is inappropriate or abusive you must report it to your line manager and also to the ICT Service Desk (to see if they can block future occurrences)
- Do not open attachments from unsolicited e-mails and do not forward such items to any other recipients under any circumstances (please delete the e-mails)
- Do not open attachments or forward e-mails that include:
    - "jokes" or other "humorous" materials
    - "chain letter" type e-mails
    - unrecognised invoices
- It is the duty of every employee to ensure that the e-mail system is used correctly
- You should not subscribe to any mailing list that will send you material that conflicts with these guidelines
- You must not forward any sensitive information to your private e-mail address (either manually or via auto-forwarding)

- Any messages or information you send outside of the council, are statements that reflect on the council. Wherever appropriate, you must make it clear that the views expressed are personal and may not necessarily reflect those of the council
- Despite putting confidential disclaimers and, where appropriate, personal disclaimers, on external communications, there is still nevertheless a legal connection to the council. Always remember that any statement you make may still be construed as representing the council
- All information systems including the e-mail system are the property of the council. In certain circumstances your line manager or another appropriate authorised Officer of the council can be provided with access to your mailbox (for example if information in your mailbox is required to deliver a service)
- Requests for access to mailboxes should be directed to the ICT Service Desk with the approval of the appropriate line manager and it is the responsibility of the line manager to ensure that access to another user's mailbox is legal (advice from the Information Assurance Manager should be sought)
- Your line manager or an appropriate authorised Officer of the council can be provided with access your mailbox and/or any other data held in electronic format for the purpose of any disciplinary investigation. In this case confidentiality of your e-mail account and/or any other relevant data cannot be given. You are therefore advised that using the councils systems for any personal use (that you intend to be confidential) is unwise
- Use of personal e-mail storage (i.e. pst or ost files) for storing e-mails outside of the corporate e-mail system is not allowed
- All requests for increased mailbox capacity should be directed to the ICT Service Desk
- Users are reminded that increased mailbox capacity is only granted if the user has accepted their obligations to perform regular e-mail "housekeeping"
- Never use the e-mail system for knowingly doing anything illegal under UK law
- Never transmit sensitive information on e-mail unless you are certain that appropriate technical controls are in use
- Never abuse others - even in response to abuse directed at you
- Never use e-mail to harass or threaten other employees, Service users or anyone in any way

- Never use anonymous mailing services to conceal your identity or falsify e-mails to make them appear to originate from someone else
- Never access anyone else's mailbox unless they have given you proxy or authorisation rights or it has been agreed by senior management (unauthorised access is a breach of security and could be subject to disciplinary action)
- Don't use the 'Reply All' function unless everyone in the original message needs to know your response
- Don't print out messages routinely
- Don't create e-mail congestion by sending trivial messages or by copying e-mails to those who don't need to see them
- Don't send 'All User' e-mails. (ICT, Communications & Marketing and a few other users can send urgent communications if required)
- Respect any handling instructions included by the e-mail sender
- Remember e-mails may be read by a far wider audience than originally intended, because of the ease of forwarding messages to new recipients
- Remember e-mail is not guaranteed to arrive at its destination within a particular time, or even at all
- Remember not to send a message in capital letters. It is the electronic version of SHOUTING
- Remember any advice you give on e-mail has the same legal standing as any other written advice
- Remember before sending an e-mail, ask yourself how you would feel if your message was read out in Court or disclosed under Freedom of Information legislation
- Remember not to assume that the message has been read just because it has been sent
- Remember you can make reasonable and occasional personal use of the system, however this will be recorded and excessive use acted upon
- Remember to avoid sending graphics - it may look nice but it takes up valuable computer storage space and increases processing time
- Do maintain your Email mailbox properly
- Make sure that an `Out of Office' message is set up if you are away from the office for more than half a day

- Do only keep messages that are necessary for current business needs
- Do store all e-mail messages necessary for permanent business records in folders agreed with your line manager and according to current record retention policies
- Do delete insignificant, obsolete and unnecessary messages, return/read receipts and attachments, daily. Clear your `deletion' folder daily to get rid of unwanted items
- Do reply promptly to all e-mail messages requiring a reply. Where a prompt detailed response is not possible, send a short e-mail acknowledging receipt and giving an estimate of when a detailed response will or should be sent
- Do develop orderly filing systems for messages you need to retain
- Do always enter a subject title to your e-mail. Make sure that the 'subject' field of the message is meaningful. This helps everyone file and search for their messages more effectively
- Do try to use one message for one subject. Multiple subjects within a single message make it more difficult for the recipient to respond effectively, and to file the message
- Do think whether all your intended recipients really want or need to receive the message and any attachments

Email signatures

- Where available you must use a signature function to set an automatic signature to the bottom of your e-mails
    - For Microsoft Outlook this can be set at: File, Options, Mail, Signatures
    - For iPads and iPhones this can be set at: Settings, Mail, Signature
    - For Windows phones this can be set at: Mail app, settings, Signature=On

- Common requirements:
    - Arial 11 point
    - Text in black, non-bold and non-italic, not on a coloured or textured background/wallpaper and doesn't include a scanned or stylised signature image

New messages:

Your name (followed by limited post-nominals & qualifications in Arial 7 point)
Your job title
Your department or service
Chesterfield Borough council

Telephone: ##### ## ####
www.chesterfield.gov.uk

Approved graphic logos only (ask PR)

Replies / forwards:

Your name (followed by limited post-nominals & qualifications in Arial 7 point)
Your job title
Telephone: ##### ## ####

The council(s) websites

- No department within the council may establish a separate internet site unless this is formally authorised by senior management

- It is important that the information contained on the council's website is both accurate and up to date. It is the responsibility of officers to ensure website content for their service areas is accurate and up to date

- The council's Communications and Marketing service is the main point of contact for all enquiries regarding the News section of the council website

Where to store data

Data should be held centrally on the relevant server(s) and will be backed-up by the ICT Service in accordance with the requirements specified in the council's Business Continuity Plan. Data should not normally be held locally on a computer as it will not be backed up.

The Employee should contact the ICT Service if there is any doubt about whether data is being held on a computer and to discuss arrangements for backing up the data.

Taking photos

- Council supplied equipment that can take photos (such as Digital Cameras, Mobile Phones, etc.) must only be used for council business (in appropriate places at appropriate times). The use of such equipment for personal purposes or for any purpose that would bring the council into disrepute is strictly prohibited
- The use of personally owned ICT equipment that can take photos should be used in accordance with the personally owned devices (BYOD) guidance

Desk policy (data protection aspects only)

- You must not leave your computer unlocked (i.e. switched on and not password protected) when you are out of sight and not in direct control of the computer
- You must not leave documents containing sensitive information unattended
- You must lock away any documents containing sensitive information when not required
- Special attention must be given to protecting any information asset that is held in an area accessible by the public

Use of social media (data protection aspects only)

- You must not participate in any discussions that are inappropriate for the council to be involved with, whether locally or nationally, and you must not give advice or information that you know to be contrary to the council's policies or interests
- You must not reveal any confidential information online in a public forum
- Employees should be aware that social networking websites are a public forum, particularly if the employee is part of a "network". Employees should not assume that their entries on any website will remain private. Employees should never send abusive or defamatory messages

- Employees must also be security conscious and should take steps to protect themselves from identity theft (and phishing attacks), for example by restricting the amount of personal information that they give out

- Social networking websites allow people to post detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords. In addition, employees should:
    - ensure that no information is made available that could provide a person with unauthorised access to the council and/or any confidential information; and
    - do not publish or report on conversations that are confidential
    - do not publish or record any confidential information regarding the council on any social networking website
    - do not disclose personal data or information about the council, or its service users, employees or managers that could breach data protection law e.g. photographs, images
    - comply with data protection, intellectual property and copyright laws

<u>Child Protection on Social media</u>

- If an employee is moderating an online chatroom, online media or overseeing any content and activity where the participants will include children under 18 the employee will need to be DBS vetted to the level of an enhanced check (with a children's barred list check if activity is more than 3 times a month)

- Employees should not publish images of children or children and adults unless consent has been given in writing by someone with parental responsibility

<u>Recruitment and social media</u>

- At no stage during the selection process will searches on prospective employees be carried out on social networking websites

<u>Intranets</u>

- The council's "aspire" intranet is encouraged to be used by personnel for electronic discussions

<u>Agile/Mobile working</u>

- The screen on devices used for home and mobile working should not be visible and easily readable by others to protect sensitive information, for example on public transport, conference centres and meeting places

- Devices used for agile, home and mobile working carrying sensitive information should not be left unattended and, where possible, should be physically locked away, or special locks should be used to secure the devices

- You should seek prior authorisation to work outside your existing established council office building where the business process needs to meet specific security requirements or sensitive information is processed
- Users processing HMRC and DWP data have additional security requirements to meet. Do not assume that if you are given a device for agile working that you have met the requirements. Contact ICT Service Desk for advice

Note to ICT: Information Security requirements for Mobile/Agile working must be implemented in accordance with the council's Information Security Policy section "Mobile Working".

Password guidelines

We aim not to over burden users with passwords. However compliance frameworks such as PCI DSS stipulate strict password requirements.

If you are not processing cardholder data or other sensitive information and are experiencing issues with too many passwords please contact the ICT Service Desk who will check if the particular system can be reconfigured with less strict authentication requirements.

We will continue to adopt changes to passwords to reflect industry best practice.

How to select strong passwords or passphrases

- To create a strong password simply choose three random words. Numbers and symbols will also need to be included to meet the password complexity requirements.
- It is important to have strong and separate passwords for each account that you use, as a compromise of one system can lead to the other system being compromised with the same password.
- Never use any word which is related to you and may be easy to guess. Absolutely never use:
    - Current partner's name
    - Child's name
    - Other family members' name
    - Pet's name
    - Place of birth
    - Favourite holiday
    - Something related to your favourite sports team
- Never use passwords which are now considered 'weak'. They include:

- “password” and variants of it: Password/P@ssw0rd
- Months of the year even if it meets the complexity rules: December2017
- Seasons of the year even if it meets the complexity rules: Summer2017
- Common keyboard sequences such as: qwerty/12345/asdf
- Common numeric sequences such as: 12345/1111/01246/

How to remember strong passwords

- There are some simple memory tricks and techniques that could help you if you’re struggling to remember your strong passwords:
    - Loci method: imagine a familiar scene and place each item that needs to be remembered in a particular location i.e. red rose on the table, book on chair, poster on wall. Imagine yourself looking around the room in a specific sequence. Re-imagine the scene and the location of each item when you need to remember it
    - Story methods: remember a sequence of key words by creating a story and including memorable details e.g. ‘the little girl wore a bright yellow hat as she walked down the narrow street…’.
- Storing passwords. Passwords can be stored as follows:
    - Write your passwords down but store them in a safe place
    - Store them in a ‘password vault’ app or application such as:
        - LastPass
        - Dashlane
        - KeePass
        - 1Password

      Note: this is not an endorsement of any password manager.
    - Store them in your web browser (but only on a computer that you have logged into with your username and not on a public/internet café computer)
- Passwords must not be stored as plain text (unencrypted) within files on electronic folders

Re-using existing passwords or passphrases

- Do not re-use previously used passwords or passphrases that you know have been compromised (on any system at home or work)

NOTE: If you process payment card transactions then PCI DSS compliance does not currently allow you to re-use previously used passwords. You therefore may be a

member of a password policy that will prevent you from re-using existing passwords. This may also be true for password policies for other information deemed sensitive.

- Use separate passwords for home and work and understand the difference between ‘high value’ and ‘low value’ accounts and passwords

- High value accounts include:

    - Your corporate active directory / email account
    - online banking and online payment services
    - password manager 17ccounts
    - work accounts used to login to ICT systems
    - cloud storage
    - platform accounts (like Apple, Microsoft or Google)
    - federated ID (where you log into one account using the credentials from another, usually Facebook or Google)
    - any account that you would be devastated to lose (for example your favourite social media accounts)

- Low value accounts could include:

    - an account that has very little personal data
    - an account that can’t be used to spend your money
    - an account that doesn’t contain any personal information about other people
    - an account where there is no expensive or irreplaceable content (like photos, music, games etc)

- Crucially, if criminals steal one of these ‘low value’ passwords, it would only give them access to other low value accounts that share the same password. Your high value accounts, all of which should have unique passwords, would still be protected

Suspicion of compromised password or passphrase

- You must immediately change your password if there is any suspicion the password could have been compromised
- If you have used the same password on multiple systems (not recommended) then you will need to change the password on all of those systems that share the common password
- Report it if you believe your password could have been compromised

Sharing passwords

- Avoid sharing your password where it is not appropriate to do so

Using Wi-Fi

- Users accessing sensitive information must not connect to public Wi-Fi hotspots or conduct business in public areas including coffee shops
- Users must not disable the corporate VPN, anti-virus settings, disable proxy settings or any other setting that have been configured to protect the device

Note to ICT: Please refer to the Information Security Policy for guidance on securing Wi-Fi.

Procedures for handling council information

Users must familiarise themselves with the guidance for classifying information and the guidance for handling information.

Cloud based systems

Cloud based systems can be defined as the use of any information system that is not hosted on the council's premises and is hosted on the internet by a third party.

- User's must ensure that they have obtained permission to use a cloud based system before processing council information on it (this is to ensure that we meet our various contractual and legal obligations)
    - this is normally met by one or more of the following tasks:
        - Request to ICT
        - Discussing with the Information Assurance Manager and/or the service provider's security team as appropriate
        - Following the council's project management procedures

Note to ICT: Cloud based systems must be implemented in accordance with the council's "Cloud security guidance". Please refer to the Information Security Policy.

Use of encryption to protect information

- Encryption should be used where possible to help protect information from unauthorised access
- ICT will normally provide encryption facilities for sending e-mails securely or sending files securely. Contact the ICT Service Desk for assistance

Note to ICT: Encryption must be implemented in accordance with the council's Encryption Guidance". Please refer to the Information Security Policy.

End user devices

- council ICT equipment must not be used for any non-work related purposes (except as noted for permitted personal use) or in any way that will bring the council into disrepute

- All ICT equipment must be located, installed and operated in line with current policies regarding health and safety at work
- It is each employee's duty to ensure that all council ICT equipment is used responsibly in undertaking their duties for the council
- Any loss or damage to council ICT equipment (including any device or media with stored data) must immediately be reported to your line manager and to the ICT Service Desk
- All old / surplus or other ICT equipment that is no longer required by a service must be notified to the ICT Service Desk for reallocation or disposal
- You must not use the council's ICT systems for anything which is illegal or any of the following actions:
    - Promoting any commercial ventures, causes or organisations unless specifically authorised to do so by your line manager
    - Promoting any private or personal interests such as selling personal possessions / property, or promoting a social activity not related to the council
    - Publishing any material that, in whole or in part, appears to be designed to affect public support for a political party. This could take the form of political publicity, campaigning or lobbying
    - Sending, accessing, retrieving or storing any communications of a discriminatory or harassing nature, or materials that are offensive, obscene, pornographic, sexually explicit, incite hatred or depict violence
    - Using or transmitting abusive, defamatory, libellous, profane or offensive language
    - Representing values which are contrary to any council policies
    - Breaking through security controls, whether on the council's equipment or on any other computer system
    - Any activities that could knowingly cause congestion and disruption of networks and systems
    - Disclosure of any personal information in breach of data protection law
- The use of ICT systems for the procurement of goods and services is only permitted where these systems are part of an approved process, with agreed audit controls

Note to ICT: End user devices must be implemented in accordance with the council's "End User Devices Security Prerequisites Guidance". Please refer to the Information Security Policy.

Using personally owned devices (Bring your own device)

Users opting to use their own devices for accessing non-sensitive council information must familiarise themselves with the guidance for use of “Personally owned end user devices”.

Please refer to the Information Security Policy section “Personally owned end user devices (Bring your own device or BYOD)”.

Note to ICT: BYOD must be implemented in accordance with the council’s guidance for using personally owned equipment. Please refer to the Information Security Policy section “Personally owned end user devices (Bring your own device or BYOD)” for ICT requirements.