Acceptable use of ICT facilities at Citizens Advice Mole Valley

This policy was adopted on: 18 November 2019

This policy was reviewed on: 04 November 2021

Next review due: 01 November 2022

Reasons for having this policy

All Citizens Advice Mole Valley's information communication technology (ICT) facilities and information resources remain the property of Citizens Advice Mole Valley and not of particular individuals, teams or departments. By following this policy, we will help to ensure that ICT facilities are used:

- legally
- securely
- effectively
- in accordance with information assurance standards
- without undermining Citizens Advice Mole Valley
- in a spirit of co-operation, trust and consideration for others
- so that they remain available

The policy relates to all information communication technology facilities and services provided by Citizens Advice Mole Valley, although special emphasis is placed on email and the internet. All members of staff and volunteers are expected to adhere to the policy.

Disciplinary measures

Deliberate and serious breach of the policy statements in this section will lead to disciplinary measures which may, for paid staff, lead to dismissal. Citizens Advice Mole Valley accepts that ICT – especially the internet and email system – is a valuable business tool. However, misuse of this facility can have a negative impact upon employee / volunteer productivity and the reputation of the service.

In addition, all of the organisation’s telephone, internet and email related resources are provided for business purposes. Therefore, the organisation maintains the right to monitor the volume of internet and network traffic, together with the email systems. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

Copyright

Take care to use software legally in accordance with both the letter and spirit of relevant licensing and copyright agreements. Copying software for use outside these agreements is illegal and may result in criminal charges.

Be aware of copyright law when using content, you have found on other organisations’ websites. The law is the same as it is for printed materials.

Security

Do not attempt to gain unauthorised access to information or facilities. The Computer Misuse Act 1990 makes it a criminal offence to obtain unauthorised access to any computer (including workstations and PCs) or to modify its contents. If you do not have access to information resources you feel you need, contact IT Support.

Do not disclose personal system passwords or other security details to other staff, volunteers or external agents, and do not use anyone else's log-in; this compromises the security of Citizens Advice Mole Valley. If someone else gets to know your password, ensure that you change it or get IT Support to help you.

If you leave your PC or workstation unattended without logging off, you are responsible for any misuse of it while you are away. Logging off is especially important where members of the public have access to the screen in your absence.

Any pen drives or other storage devices used on the local Citizens Advice network should be secure and the property of the local Citizens Advice. No staff / client personal data should be held on a pen drive unless it is suitably encrypted to FIPS 140 standard as explained in the CABlink guidelines

Information about people

If you are recording or obtaining information about individuals, make sure you are not breaking data protection legislation. When you are on the internet and using email, make sure your actions are in the interest (and spirit) of Citizens Advice Mole Valley and do not leave Citizens Advice Mole Valley open to legal action (for example libel). Avoid trading insults over the internet.

Obscenities / pornography

Do not write it, publish it, look for it, bookmark it, access it or download it.

Electronic monitoring

You may find that you have access to electronic information about the activity of colleagues. Any such information must not be used by unauthorised individuals to monitor the activity of individual staff in any way (e.g. to monitor their working activity, working time, files accessed, internet sites accessed, reading of their email or private files etc.) without their prior knowledge. Exceptions are:

- In the case of a specific allegation of misconduct, when the Management Team can authorise accessing of such information when investigating the allegation.
- When IT Support cannot avoid accessing such information while fixing a problem.

In the former case, access to ICT facilities may be disabled pending an investigation.

Client data using Casebook

When you are recording or obtaining information about individuals, make sure you are not breaking data protection legislation. When you are using Casebook make sure your actions are in the interest of Citizens Advice Mole Valley.

Casebook contains sensitive client information. You should:

- Only access client information for the purposes of doing your job.
- Only access the minimum amount of information necessary to complete your task.
- Understand that use of Casebook is monitored and audited to ensure that people are accessing information for the right reasons, at the right time.

Misuse of client information is a breach of confidentiality and may result in disciplinary action, or contract termination. Misuse of client information can be a criminal offence under Section 55 of the Data Protection Act and will be reported to the police.

Access to client data

Client data should only be accessed when you have a business reason to do so. Only access the minimum amount of data that you need to carry out the business task. Casebook has audit trails for usage to ensure that people are accessing data to fulfil required business needs only. Only view, create or add to client records if you have a valid business need. Regular reports will highlight usage of Casebook within Citizens Advice Mole Valley. Any client record of another LCA viewed or accessed will be registered and reported, a regular audit of these reports will be undertaken to ensure appropriate use.

Collaborating LCA

When Citizens Advice Mole Valley has a recognised partnership e.g. Adviceline, and there is a valid business need to view, create or add to the client record that belongs to other LCA in the group it is permissible to do so.

Instances of misuse will be investigated and dealt with appropriately. Any breaches of policy or confidentiality will be taken very seriously indeed: for staff, this may result in disciplinary action; for volunteers or contractors, if the impact is serious enough, this may mean it is no longer appropriate for them to work in the service. Some breaches of confidentiality are criminal offences under Section 55 of the Data Protection Act.

Sensitive data

You should be aware of sensitive data and always seek advice from the Information Asset Owner when dealing with sensitive data.

Ensure that sensitive data is always stored securely; do not hold copies of sensitive information away from Casebook unless you have the permission of the Information Asset Owner.

Sharing data

Do not discuss or release data into the public domain. If there is a business need to share data, seek agreement from the Casebook Information Asset Owner. Any data shared will need to be done in accordance with the Data Sharing Agreement.

Conflict of interest checks on clients

You are permitted to search for a client across the whole service database if there is a business need. Finding the client does not create a conflict of interest. You should not open the enquiry record to check whether a conflict exists after finding the relevant client - please refer to Policy on accessing case records on Casebook for guidance.

Reports

If you are responsible for Casebook reports, ensure that you only download the minimum amount of data needed. If the reports contain personal data and are exported to another document, you need to make sure that this document is kept in a secure location which can only be accessed by people who have a business need to use it and is preferably encrypted or password protected.

Printing

If you have access to printing within Casebook, only print the minimum amount of data needed; ensure that you are near the printer to be able to collect it immediately. Store the printed information securely until you can dispose of it securely (see Golden rules of keeping data safe).

Casebook user names and passwords

Users must only access Casebook using their own user identification and password. Do not tell anybody else your username and password. Do not write your username and password down. Change your password when prompted. Seek agreement from the Casebook Administrator and Information Asset Owner for Casebook if you have a business need to share your details. Ensure your password is changed immediately afterwards.

Locking your computer

In all instances it is recommended that your screen is locked if you leave your workstation. If Casebook is available you must lock your screen if you are not present (Ctrl, Alt, Del).

Logging out of Casebook

Ensure that you log out of Casebook when you are away from your workstation for a significant amount of time. You should ensure that all browser windows are closed before logging out.

Training and awareness

All members of Citizens Advice Mole Valley should complete annual information assurance training appropriate to their role at CAMV and be familiar with CAMV policies. Management will support you in this, and any concerns should be raised with a manager. Golden rules of keeping data safe is available on CABlink and BMIS and provides practical guidance on keeping data secure.

Awareness: you must remain aware of who may see your screen when dealing with client information. Always be aware of the physical location you are working in and report any unexpected visitors or instances. When working away from the bureau, ensure your device is encrypted if it contains personal data. Keep your equipment with you at all times.

Information assurance incidents

All incidents involving client or CA sensitive data should be reported to the IAO, if you are aware of another member of staff behaving inappropriately concerning Casebook (and anything else) speak to your manager or use the whistleblowing policy.

Email

When to use email

Use email in preference to paper to reach people quickly (saving time on photocopying / distribution) and to help reduce paper use.

Emailing client / personal details

Client or staff personal should not be emailed unless a suitable encryption product is used. If in doubt ask the Information Assurance Officer in the local Citizens Advice.

Use the phone for urgent messages (email is a good backup in such instances). Use of email by employees / volunteers of Citizens Advice Mole Valley is permitted and encouraged where such use supports the goals and objectives of the service / charity.

At Citizens Advice Mole Valley, it is expected that all email users will ensure that they:

- comply with current legislation
- use email in an acceptable way
- do not create unnecessary business risk to the local Citizens Advice by their misuse of the internet.

Unacceptable behaviour

- Sending confidential information to external locations.
- Distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal.
- Distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment or bullying.
- Using copyrighted information in a way that violates the copyright.
- Breaking into the local Citizens Advice's or another organisation's system, or unauthorised use of a password / mailbox.
- Broadcasting unsolicited personal views on social, political, religious or other non business-related matters.
- Transmitting unsolicited commercial or advertising material.
- Undertaking deliberate activities that waste staff effort or networked resources.
- Introducing any form of computer virus or malware into the corporate network.
- Emailing client / staff details without suitable encryption.

Confidentiality

Always exercise caution when committing confidential information to email, since the confidentiality of such material cannot be guaranteed. Citizens Advice Mole Valley reserves the right to monitor electronic communications in accordance with applicable laws and policies. The right to monitor communications includes messages sent or received by system users (employees, volunteers and temporary staff) within and outside the system as well as deleted messages.

General points on email use

When publishing or transmitting information externally be aware that you are representing Citizens Advice Mole Valley and could be seen as speaking on Citizens Advice Mole Valley's behalf. Make it clear when opinions are personal. If in doubt, consult your line manager.

Check your inbox at regular intervals during the working day. Keep your inbox fairly empty so that it just contains items requiring action.

Try to decide what to do with each email as you read it (e.g. delete it, reply to it, save the whole email in a folder, or extract just the useful information and save it somewhere logical).

Keep electronic files of electronic correspondence, only retaining what you need to. Do not print it off and keep paper files unless absolutely necessary.

Treat others with respect and in a way in which you would expect to be treated yourself (e.g. do not send unconstructive feedback, argue, or invite colleagues to make public their displeasure at the actions / decisions of a colleague).

Do not forward emails warning about viruses (they are invariably a hoax and IT Support will probably already be aware of genuine viruses – if in doubt, contact them for advice).

Do not open email unless you have a reasonably good expectation of what it contains, and do not download files unless they are from a trusted source, e.g. do open **report.doc** from a colleague you know. Do not open **explore.zip** sent from an address you have never heard of, however tempting. Alert IT Support if you are sent any unsolicited messages. This is one of the most effective means of protecting Citizens Advice Mole Valley against email virus attacks.

Internet use

Use of the internet by employees and volunteers of Citizens Advice Mole Valley is permitted and encouraged where such use supports the goals and objectives of the business.

However, Citizens Advice Mole Valley has a policy for the use of the internet whereby employees and volunteers must ensure that they:

- comply with current legislation
- use the internet in an acceptable way
- do not create unnecessary business risk to the company by their misuse of the internet.

Unacceptable behaviour

In particular the following is deemed unacceptable use or behaviour by employees and volunteers:

- Visiting internet sites that contain obscene, hateful, pornographic or other illegal material.
- Using the computer to perpetrate any form of fraud, or software, film or music piracy.

- Using the internet to send offensive or harassing material to other users.
- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence.
- Hacking into unauthorised areas.
- Creating or transmitting defamatory material.
- Undertaking deliberate activities that waste staff effort or networked resources.
- Introducing any form of computer virus into the corporate network.

Social media

For the purposes of this policy, social media websites are web-based and mobile technologies which allow parties to communicate instantly with each other or to share data in a public forum. They include websites such as Facebook, Twitter, Google+ and LinkedIn. They also cover blogs and image sharing websites such as YouTube and Flickr. This is not an exhaustive list and you should be aware that this is a constantly changing area.

Use of social media at work

Employees and volunteers are permitted to make reasonable and appropriate use of social media websites from the local Citizens Advice's IT equipment. You should ensure that usage is not excessive and does not interfere with work duties.

Use should be restricted to your non-working hours, unless this forms part of your work responsibilities.

Access to particular social media websites may be withdrawn in the case of misuse.

Monitoring use of social media websites

Citizens Advice Mole Valley maintains the right to monitor usage where there is suspicion of improper use.

Social media in your personal life

Inappropriate comments on social media websites can cause damage to the reputation of Citizens Advice Mole Valley if a person is recognised as being an employee or volunteer of the Citizens Advice service. It is, therefore, imperative that you are respectful at all times towards the Citizens Advice service, including clients, colleagues, partners and competitors.

Citizens Advice Mole Valley volunteers, trustees and paid staff should not give the impression that they are representing, giving opinions or otherwise making

statements on behalf of the Citizens Advice service, unless appropriately authorised to do so.

Personal opinions must be acknowledged as such, and should not be represented in any way that might make them appear to be those of Citizens Advice Mole Valley. Where appropriate, an explicit disclaimer should be included, for example: '*These statements and opinions are my own and not those of Citizens Advice Mole Valley.'*

Any communications that local Citizens Advice workers make in a personal capacity must not:

- bring the local Citizens Advice into disrepute, for example by criticising clients, colleagues or partner organisations
- breach the local Citizens Advice's policy on client confidentiality or any other relevant policy, such as Information Assurance.
- breach copyright, for example by using someone else's images or written content without permission (note that logos and trademarks cannot be used without the consent of Citizens Advice)
- do anything which might be viewed as discriminatory against, or harassment towards, any individual, for example, by making offensive or derogatory comments relating to: age, disability, gender reassignment, race, religion or belief, sex, or sexual orientation
- use social media to bully another individual, such as a co-worker
- post images that are discriminatory or offensive (or links to such content)

Personal use of ICT

Use of facilities for leisure or personal purposes (e.g. sending and receiving personal email, personal phone calls, playing computer games and browsing the internet) is permitted so long as such use does not:

- incur specific expenditure for Citizens Advice Mole Valley
- impact on your performance of your job or role (this is a matter between each member of staff or volunteer and their line manager)
- break the law
- bring Citizens Advice Mole Valley into disrepute
- detrimentally affect the network performance by using large amounts of bandwidth (for instance by downloading / streaming of music or videos)
- impact on the availability of resources needed (physical or network) for business use.

Any information contained within the local Citizens Advice in any form (e.g. AdviserNET) is for use by the volunteer or employee for the duration of their period of work and should not be used in any way other than Citizens Advice business, or transferred into any other format (e.g. loaded onto a memory stick / pen drive).

Miscellaneous

Hardware and software

The Manager should approve all purchases, preferably through the ICT budget.

Laptops and mobile devices

Equipment, data, information sources or software must not be taken off-site by members of staff or volunteers without documented management authorisation. (Management may provide authorisation on a ‘once only’ basis as long as it is subject to regular review).

Laptops and mobile devices must have appropriate access protection, i.e. passwords and encryption and must not be left unattended in public places.

Laptops and mobile devices are vulnerable to theft, loss or unauthorised access. Always secure laptops and mobile devices when leaving an office unattended. When travelling, the high incidence of car theft makes it inadvisable to leave laptops and mobile devices in cars or to take them into vulnerable areas.

To preserve the integrity of data, frequent transfers must be maintained between laptops and mobile devices and the main file system. Laptops and mobile devices must be maintained regularly and batteries recharged regularly.

Users of laptops and mobile devices are responsible for the security of the hardware and the information it holds at all times, on or off local Citizens Advice property.

The equipment should only be used by the person to whom it is issued. All of the policy statements regarding the use of ICT apply equally to users of portable equipment.

Users of laptops and mobile devices are advised to check their car and home insurance policies for their level of cover in the event of equipment being stolen or damaged, and take appropriate precautions to minimise risk of theft or damage.

Care should be taken when working on laptops in public places (e.g. trains) that any client / staff details are not visible to other people.

Remote access

Remote access by employees or volunteers or other trusted parties on to the Citizens Advice network should be individually approved, and must be by a recognised and approved method such as VPN RAS access.

Installing software

Get permission from IT Support before you install any software (including public domain software) on equipment owned and / or operated by Citizens Advice Mole Valley.

Data transfer and storage on the Citizens Advice network

Keep master copies of important data on Citizens Advice Mole Valley's network server and not solely on your PC's local C: drive or portable discs. Otherwise it will not be backed up and is therefore at risk.

Ask for advice from IT Support if you need to store, transmit or handle large quantities of data, particularly images or audio and video. These large files use up disk space very quickly and can bring the network to a standstill.

Be considerate about storing personal (non-Citizens Advice Mole Valley) files on Citizens Advice Mole Valley's network.

Do not copy files that are accessible centrally into your personal directory unless you have good reason (i.e. you intend to amend them or you need to reference them and the central copies are to be changed or deleted) since this uses up disk space unnecessarily.

Care of equipment

Do not rearrange the way in which equipment is plugged in (computers, power supplies, phones, network cabling, modems etc.) without first contacting IT Support.

Please note:

All employees, volunteers, contractors or temporary staff who have been granted the right to use Citizens Advice Mole Valley's ICT systems are required to sign both a confidentiality declaration and this agreement confirming their understanding and acceptance of these two policies prior to any access or usage.

Acceptable use of ICT facilities at Citizens Advice Mole Valley

Agreement

All employees, volunteers, contractors or temporary staff who have been granted the right to use the company's ICT systems are required to sign this agreement confirming their understanding and acceptance of this policy.

In addition, you are required to sign a separate confidentiality declaration.

Signed:		**Signed:**	
Manager:		**Name & role**	
Date:		**Date:**	