CITIZENS ADVICE REIGATE AND BANSTEAD ACCEPTABLE USE OF ICT FACILITIES POLICY

1. Introduction

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

- legally
- securely
- effectively
- in accordance with information assurance standards
- without undermining Citizens Advice Reigate and Banstead
- 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 Reigate and Banstead, although special emphasis is placed on email and the internet. All staff and volunteers are expected to adhere to the policy.

2. Disciplinary measures

Deliberate and serious breach of the policy statements in this section will lead to disciplinary measures which may lead to paid staff dismissal. Citizens Advice Reigate and Banstead accept 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 or volunteer productivity and the reputation of the service.

In addition, all of Citizens Advice Reigate and Banstead's phone, internet and email related resources are provided for business purposes. Therefore, Citizens Advice Reigate and Banstead 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.

3. Copyright

All staff and volunteers should 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.

4. Security

4.1 Unauthorised access

All staff and volunteers should 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 your manager or supervisor or IT Support.

4.2 Passwords

All staff and volunteers should not disclose personal system passwords or other security details to other staff, volunteers or external agents, and should not use anyone else's log-in as these actions would compromise the security of Citizens Advice Reigate and Banstead. If

someone else learns your password, ensure that you change it or request IT Support to help you.

4.3 Logging off
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 if there is an opportunity for members of the public have access to the screen in your absence.

4.4 Pen drives, USBs and other storage devices
Any pen drives, USBs or other storage devices used on Citizens Advice Reigate and Banstead's network should be secure and the property of Citizens Advice Reigate and Banstead. No staff or 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

5. Information about people
If you are recording or obtaining information about individuals, make sure you are not breaking Data Protection legislation. When using the internet or email, make sure your actions are in the interest (and spirit) of Citizens Advice Reigate and Banstead and do not leave Citizens Advice Reigate and Banstead open to legal action (for example libel). Carefully construct your language when communicating electronically so as to avoid any dialogue that may be perceived as an insult.

6. Obscenities / pornography
Staff and volunteers should not write, publish, look for, bookmark, access or download obscenities or pornography it at any time or in any circumstances.

7. Electronic monitoring
Electronic information about the activity of colleagues should not be accessed or 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 case of the former, access to ICT facilities may be disabled pending an investigation.

8. Casebook use
8.1 Access
Casebook contains sensitive client information. Staff and volunteers should:

- Only access client information for the purposes of doing the task in hand.
- 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 the Data Protection Act 2018 and will be reported to the police.

8.2 Casebook usernames and passwords

- You must only access Casebook using your own username and password.
- Do not tell anybody else your username and password.
- Do not write your username and password down.

8.3 Reports

If you run Casebook reports, you must download the minimum information needed. If a report contains personal information and is exported to another document, you must make sure that this document is kept secure

9 Training

All staff and volunteers should complete annual information assurance training appropriate to their role. Management will support you in this, and any concerns should be raised with a manager. Golden rules of keeping data safe provide practical guidance on keeping data secure.

10 Personal data

You should be aware of personal data and always seek advice from a manager when dealing with personal data. Ensure that personal data is always stored securely; do not hold copies of personal information away from Casebook unless you have the permission of a manager.

11 Sharing data

Do not discuss or release data into the public domain. If you need to share data to do your job, you should have agreed processes in place.
If you are sharing personal data, this must be done in accordance with the Data Protection Act 2018, General Data Protection Regulation (GDPR), and the Membership Agreement.

12. Printing

- Only print the minimum amount of information needed
- Remove prints from the printer immediately.
- Store the printed information securely until you can dispose of it securely.

13. Locking your computer

Remember to lock your computer when you leave your workstation (Ctrl, Alt, Del for Windows computers).

14. Awareness

- Be aware of who may see your screen when dealing with client information.

15. Information assurance incidents

- All incidents involving personal data should be reported to the Information Asset Owner/manager and to Citizens Advice
- If you are aware of another member of staff behaving inappropriately concerning Casebook (or anything else) speak to your manager.

16. Email

16.1 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.

16.2 Emailing personal details

Client or staff personal data should not be emailed unless a suitable encryption product is used (for example by ensuring that the personal data is contained in an encrypted attachment (e.g. password protected Word document) rather than in the body of the email, with the password to the attachment communicated in a completely different way, for example by phone or fax).

If in doubt ask the Information Assurance Officer in Citizens Advice Reigate and Banstead.

Use the phone for urgent messages (email is a good backup in such instances). Use of email by staff and volunteers of Citizens Advice Reigate and Banstead is permitted and encouraged where such use supports the goals and objectives of the service.

However, Citizens Advice Reigate and Banstead have a policy for the use of email whereby staff and volunteers must ensure that they:

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

16.3. 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 Citizens Advice Reigate and Banstead'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.

16.4. Confidentiality

Always exercise caution when committing confidential information to email, because the confidentiality of such material cannot be guaranteed. Citizens Advice Reigate and Banstead reserve 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, ie, staff, temporary staff and volunteers within and outside the system as well as deleted messages.

16.5 General points on email use

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

Check your inbox at regular intervals during the working day. Keep your inbox fairly empty so that it only contains items requiring your 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 hoaxes 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 received unsolicited material of this nature. This is one of the most effective means of protecting Citizens Advice Reigate and Banstead against email virus attacks.

17. Internet use

17.1 When to use the internet

Use of the internet by staff and volunteers of Citizens Advice Reigate and Banstead is permitted and encouraged where such use supports the goals and objectives of the business.
However, Citizens Advice Reigate and Banstead have a policy for the use of the internet whereby staff 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.

17.2 Unacceptable behaviour

In particular the following is deemed unacceptable use or behaviour by staff 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.

18. 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 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.

18.1 Use of social media at work

18.1 When to use Social media
Staff and volunteers are permitted to make reasonable and appropriate use of social media websites from Citizens advice Reigate and Banstead'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.

18.2 Monitoring use of social media websites

Citizens Advice Reigate and Banstead maintains the right to monitor usage where there is suspicion of improper use.

18.3 Social media in your personal life

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

Citizens Advice Reigate and Banstead staff and volunteers 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 the Citizens Advice Reigate and Banstead. Where appropriate, an explicit disclaimer should be included, for example: '*These statements and opinions are my own and not those of Citizens Advice Reigate and Banstead.'*

Any communications that Citizens Advice Reigate and Banstead staff and volunteers make in a personal capacity must not:

bring the Citizens Advice Reigate and Banstead into disrepute, for example by criticising clients, colleagues or partner organisations

- breach the Citizens Advice Reigate and Banstead 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).

19. 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 Reigate and Banstead
- impact on your performance of your job or role (this is a matter between each member of staff or volunteer and their line manager or supervisor)
- break the law
- bring Citizens Advice Reigate and Banstead 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 Citizens Advice Reigate and Banstead 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).

20. Miscellaneous

20.1 Hardware and software

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

20.2 Laptops and mobile devices
Equipment, data, information sources or software must not be taken off-site by 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 Citizens Advice Reigate and Banstead 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 or staff details are not visible to other people.

20.3 Remote access
Remote access by staff and 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.

20.4 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 Reigate and Banstead.

20.5 Data transfer and storage on the Citizens Advice network
Keep master copies of important data on Citizens Advice Reigate and Banstead'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 Reigate and Banstead) files on Citizens Advice Reigate and Banstead'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.

20.6 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.

20.7 Agreement
All staff, 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.

Signed:		**Signed:**	
Manager:		**Employee or volunteer:**	
Date:		**Date:**	