CITIZENS ADVICE REIGATE AND BANSTEAD HOME AND MOBILE WORKING POLICY

1. Introduction

Citizens Advice Reigate and Banstead has a duty of care to our clients to protect the information supplied to or collected by staff and volunteers when delivering our service when working:

- At home
- At an outreach location
- At events or conferences
- At the offices of, or with, partner organisations
- While traveling
- At any other location which is not an office of Citizens Advice Reigate and Banstead

This policy applies to information in all formats, including manual records (your written notes and printouts) and electronic data.

2. Data protection

Citizens Advice Reigate and Banstead retains responsibility for complying with data protection requirements and, under data protection legislation, is responsible for the personal data which staff and volunteers process. You must therefore follow any existing data protection policies in conjunction with this policy and, in particular, ensure that no unauthorised third party has access to manual records or electronic data relating to your work for Citizens Advice Reigate and Banstead.

3. Security

In order to help you work from home or in a mobile way securely:
All laptop hard disks and mobile devices are encrypted and password protected using industry recognised encryption

- In the event of theft, loss or damage which prevents use to any laptop, mobile device or manual records (for example, a folder of records is water or fire damaged), full details should be supplied to your manager and the incident reported to Citizens Advice immediately.
- No client personal data should be saved on the laptop's hard disk
- No external storage device (flash media etc) is to be used unless provided by Citizens Advice Reigate and Banstead. Such devices must be encrypted and password protected
- Only connect your devices to secure WiFi networks. If possible configure your device not to connect automatically to unknown networks
- Never leave a device logged on when unattended and ensure that the device automatically locks if inactive for a period of time
- Take the minimum amount of sensitive data needed and record what you take so it is possible to identify whether anything has been lost. Make sure this is kept secure at all times
- Only those phones supplied or approved by Citizens Advice Reigate and Banstead are to used for any work related usage
- No clients are to be contacted using their personal landline or mobile
- Any manual records which contains personal information to be returned to Citizens Advice Reigate and Banstead for secure storage within 48 hours of creation – unless otherwise agreed, any handwritten notes to be shredded at the end of the session using the shredders provided by the local office.

Take sensible steps to protect our technology

- Don’t leave laptops open and be careful when travelling or using technology in public.
- You must take reasonable care to minimise the risk of theft or damage, and any ICT equipment
- During the transfer of equipment between home and work, you should keep the equipment in sight and not leave it unattended at any time, unless stored out of sight in a locked car, with the alarm set (if there is one).
- ICT equipment must not be left in your car overnight and you must take all reasonable steps to minimise the visibility of any such equipment, securing windows and doors when your home is unoccupied.
- All members of staff and volunteers should ensure that they are fully up to date with information security and data protection training.

4. Annual Leave and when ending employment or volunteering

Unless otherwise agreed with a manager any technology provided by Citizens Advice Reigate and Banstead or manual records such as notebooks and printouts are to be returned to the office on the last working day before the following:

- Extended Annual Leave or sabbaticals
- The end of employment or when ceasing to continue volunteering