CITIZENS ADVICE REIGATE AND BANSTEAD INFORMATION RISK POLICY

This policy has been updated for GDPR

1. Leadership and governance of information

1.1 Risks

Citizens Advice Reigate and Banstead are Data Controller of all personal data we process and Joint Data Controller with Citizens Advice (CitA) for all client information held on systems provided by CitA. Citizens Advice Reigate and Banstead use 'consent' or 'legitimate interests' as the lawful basis for processing client information. Citizens Advice Reigate and Banstead have considered its appetite for information risks and have agreed it is low. All decisions on how to manage information risks within Citizens Advice Reigate and Banstead are derived from its wish to maintain a maximum low level of risk and are overseen by the Trustee board.

1.2 Roles

Citizens Advice Reigate and Banstead have allocated specific roles with information governance responsibilities including Richard Hoffman Senior Information Risk Owner (SIRO), Andrea Dunhill, Information Asset Owner and Data Protection Officer David De Cintra. These roles provide a clear structure for the strategic governance and operational management of information risks within Citizens Advice Reigate and Banstead.

The Trustee Board oversee the effectiveness of the information risk policy and are responsible for ensuring improvements are made where necessary.

1.3 Statement of internal control

Each year, Citizens Advice Reigate and Banstead describe our approach to managing information risks within Citizens Advice Reigate and Banstead in its statement of internal control. This includes a summary report on levels of compliance with the information risk policy and whether the policy itself is sufficiently effective.

1.4 Review of risk policy

Citizens Advice Reigate and Banstead ensure the information risk policy is reviewed so that it remains comprehensive and effective at the following intervals: a) annually b) whenever significant amendments or additions are required (e.g. by changes in law or other compliance obligations) and c) after a data loss incident, if required.

All significant information processes and decisions are documented in Data protection impact assessments after consultation with information governance role holders. Risks are documented in section 11 of the Citizens Advice Reigate and Banstead Risk Assessment Grid which is reviewed at regular intervals by the Trustee Board.

2. Information risk management

2.1 Responsibilities of The Senior Information Risk Officer

The Senior Information Risk Officer (SIRO) of Citizens Advice Reigate and Banstead is responsible for ensuring the information risk policy is implemented. The SIRO is also responsible for ensuring that all significant information risks are considered, managed and documented. The SIRO will gather together an appropriate team of individuals to perform these tasks and will refer more important and/or more complex decisions to the Trustee Board as appropriate.

2.2 Data protection impact assessment

SIRO approval is required before proceeding with any activity likely to generate a significant information risk to Citizens Advice Reigate and Banstead. The decision whether to accept, avoid, transfer or mitigate against the likelihood or impact of an information risk will be based upon the information provided a in a Data protection impact assessment, together with consideration of Citizens Advice Reigate and Banstead defined risk appetite.

Citizens Advice Reigate and Banstead have adopted the Data protection impact assessment to perform information risk assessments. CitA is responsible for information risk assessments for IT systems it provides to store and process client information. Citizens Advice Reigate and Banstead authorise employment of specialist consultants to perform complex risk assessments, if required.

All information risk decisions, actions, progress and risk assessments will be recorded for reference, education and compliance purposes.

2.3 Incident management policy
Citizens Advice Reigate and Banstead have adopted the incident management policy to manage any data security incidents and to help prevent the likelihood of incidents recurring. These are supported by CitA. Citizens Advice Reigate and Banstead report all data security incidents to CitA as soon as they are detected and where required to the Information Commissioner's Office within 72 hours.

3. Data handling through life Information Governance measures
3.1 Acceptable use
Citizens Advice Reigate and Banstead ensure that all staff and volunteers read and sign its Acceptable use of ICT Facilities, prior to being given access to confidential information, including Casebook and all forms of social media. Compliance is mandatory and may be actively monitored. Any individual who fails to comply may be subject to the disciplinary or managing performance procedures set out in our staff and volunteer policies.

Citizens Advice Reigate and Banstead review its Acceptable use of ICT Facilities Policy regularly to ensure they are kept up to date.

3.2 Access control
Citizens Advice Reigate and Banstead employ the ‘need to know’ principle of minimised access to confidential data, set out in the Cabinet Office’s ‘Minimum Data Handling Measures’ when providing access to confidential data. This ensures that all staff and volunteers only ever have access to the minimum amount of confidential data required to perform their valid business role and for which appropriate consent or other lawful basis exists.

Citizens Advice Reigate and Banstead implement the ‘need to know’ access principle through the establishment of effective ICT user account management processes; by limiting the number and use of privileged accounts and by monitoring the use of ICT systems and limiting access to other physical areas which house confidential data.

3.3 Data classification
Citizens Advice Reigate and Banstead ensure that all staff and volunteers can easily identify confidential data by clearly labelling the document in the header as ‘CONFIDENTIAL’
3.4 Data in transit: email, fax, post
Citizens Advice Reigate and Banstead ensure via initial and refresher training that all

staff and volunteers understand that Citizens Advice Reigate and Banstead is legally responsible for the security of data sent whilst in transit, including but not limited to data sent via email, webchat, video, mobile applications and post. We ensure that any email containing confidential information is adequately secured by adopting the CitA recommended secure email procedures or by posting original documents using recorded Royal Mail delivery.

3.5 Retention, deletion and secure disposal
The Citizens Advice Reigate and Banstead Retention policy is followed for all client records and other individual records and mark for deletion at the end of the retention period. Citizens Advice Reigate and Banstead record retention periods on the Information Asset Register. Citizens Advice Reigate and Banstead ensure that all copies of confidential data are securely erased or destroyed at the end of their business 'life' by the use of approved services such as secure paper shredding or digital media destruction and that this can be evidenced with certificates

3.6 Removable media
Citizens Advice Reigate and Banstead mitigate against the high risks of potential data loss associated with the use of removable media (laptops, USB sticks, DVDs, CDs etc.) by avoiding the use of removable media wherever possible and, where its use cannot be avoided, by ensuring that media is adequately encrypted with a secure password.

3.7 Personal data in the cloud or externally hosted
Citizens Advice Reigate and Banstead do not store personal data in the cloud or externally. If, in the future, personal data would be stored or processed externally a data protection impact assessment will be undertaken and the ICO Cloud Computing guidance would be followed. A written 'data processing agreement' would be signed with the supplier.

3.8 ICT
Citizens Advice Reigate and Banstead implements any necessary IT Security as set out in National Cyber Security Centres 10 steps to Cyber security and uses the CitA IT Health check to help identify and action any improvements that may be required. Citizens Advice Reigate and Banstead ensure that only local CitA authorised ICT equipment and media will be used to handle, transport, store or process personal data. Privately owned ICT equipment is not used unless approved in advance by the SIRO and is subject to this policy. Citizens Advice Reigate and Banstead ensure that any remote computer processing protected personal data is protected with user logon and password that acts as an identification and authentication mechanism. Citizens Advice Reigate and Banstead avoids the use of live or identifiable data in system testing.

3.9 Physical security
Citizens Advice Reigate and Banstead protect the physical locations where confidential data is held using a number of layers of security defined in the physical security checklist. Citizens Advice Reigate and Banstead ensure that each staff member or volunteer receives initial and refresher training to confirm they understand the importance of their role in maintaining the 'layers' of physical security that they have control over – as no single person controls all elements, teamwork is essential.

3.10 Home working and mobile working

Citizens Advice Reigate and Banstead ensure all staff and volunteers receive training to understand their personal responsibilities relating to confidential data when

working from home and in outreach locations which are defined in the Homeworking Policy and Outreach Policy]. Compliance is mandatory and will be actively monitored. Any individual who fails to comply may be subject to the disciplinary or managing performance procedures set out in the staff and volunteer policies.

3.11 Assured information sharing
Citizens Advice Reigate and Banstead will put in place data sharing or processing agreements consistent with the ICO's Code of Practice on Data Sharing where the business need to share confidential data with external organisations exists and where consent or other legal authority exists for the data sharing. This will be either in specific contracts or by use of a data processing or data sharing agreement. Case-level data sharing or referral will be recorded on Casebook.

3.12 Location of personal information
Citizens Advice Reigate and Banstead identifies where all personal data is processed and stored and aims to keep this within the UK or within Europe. If, in the future, data is to be processed outside Europe, for example by a US based cloud services provider, there must be reference as to how security requirements for this type of transfer are met stated within in a written contract or data processor agreement.

4. Individual rights
4.1 The right to be informed

Citizens Advice Reigate and Banstead provide appropriate information to its clients across all channels through appropriate privacy notices and just in time notices.

Citizens Advice Reigate and Banstead describe what information is being collected, who is collecting it, how and why is it collected and how it is used and shared. Citizens Advice Reigate and Banstead follow the ICO guidance. Citizens Advice Reigate and Banstead allow members of the public to contact our service by providing clear contact details to exercise their personal data rights such as:

- the right to request copies and access of the personal information we hold including the option to modify the consent they have given;
- the right to request appropriate rectification of any inaccuracies or incomplete information of their personal data;
- the right to erasure (where appropriate) or anonymization;
- the right to restrict or stop processing where appropriate;
- the right to data portability where appropriate

4.2 automated decision making or profiling
Citizens Advice Reigate and Banstead does not use automated decision making or profiling

5. Compliance
Citizens Advice Reigate and Banstead ensure that confidential data assets are managed properly by documenting its information assets in an Information Asset Register. Citizens Advice Reigate and Banstead ensure that the data flows of information for that asset are known and documented ensuring data protection impact assessments are carried out in high risk areas.

Each asset has an Information Asset Owner designated who has responsibility for the security and business use of the asset.

Citizens Advice Reigate and Banstead employ joining and leaving checklists to ensure that confidential data assets are returned and access to any information is removed when someone leaves.

Citizens Advice Reigate and Banstead ensure all staff, volunteers and contractors successfully complete appropriate data protection training and are made aware of the importance Citizens Advice Reigate and Banstead places upon looking after the confidential data entrusted to it. This training is carried out prior to being given access to confidential information and this is refreshed at least annually. Roles with additional responsibilities, such as Information Asset Owners, are additionally required to successfully complete advanced training. Successful completion of training is documented and monitored by the Training Manager. Failure to comply is escalated to the SIRO, and if necessary the Trustee Board, until resolved.

Citizens Advice Reigate and Banstead ensure our staff and volunteer policies are kept up to date to help implement effective management of information risks. The Acceptable use of ICT Facilities Policy requires all staff and volunteers to keep confidential data safe.

All staff and volunteers received training so they know that data security breaches caused by their actions may result in disciplinary or equivalent volunteer proceedings which in some cases may be considered gross misconduct, and that some instances may be criminal offences under the Data Protection Act 2018 or legislation equivalent to the General Data Protection Regulation. All staff and volunteers, including contractors, sign confidentiality or non-disclosure agreements prior to being given access to confidential data.

Citizens Advice Reigate and Banstead regularly review audit information for its main ICT systems to ensure that access to confidential data complies with the Acceptable use of ICT Facilities Policy. Any potentially suspicious activity is investigated and remedial actions taken where necessary and this may include retraining or disciplinary proceedings.

Citizens Advice Reigate and Banstead implement a Whistleblowing Policy which allows any staff member or volunteer to raise concerns about information risks, anonymously if necessary, so that these can be investigated and steps taken to adequately address any legitimate matters.

Citizens Advice Reigate and Banstead will implement appropriate contractual requirements relating to data protection and information security as required by our funders and partner organisations.

Citizens Advice Reigate and Banstead comply with any mandatory elements of the CitA Membership Agreement and Membership Scheme relating to the management of information risk which includes any reasonable measures to allow legal compliance to the General Data Protection Regulation (GDPR).