CAMV Information Risk Policy

This policy was adopted on:	18 November 2019
This policy was reviewed on:	01 October 2021
Next review due:	01 October 2022

Leadership and Governance

We, the Trustee Board of Citizens Advice Mole Valley (CAMV) are the Data Controller of all the personal data we process and Joint Data Controller with Citizens Advice for all client information held on systems provided by Citizens Advice. We use 'consent' or 'legitimate interests' as our lawful basis for processing client information. We have considered our appetite relating to information risks and have agreed it is medium. All decisions on how to manage information risks within CAMV are derived from our wish to maintain a maximum low level of risk.

We have allocated specific roles with information governance responsibilities across CAMV including Senior Information Risk Owner, Information Asset Owner(s) and Data Protection Officer (DPO) if appropriate. These roles provide a clear structure for the strategic governance and operational management of information risks within CAMV.

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

Each year, we describe our approach to managing information risks within CAMV in our statement of internal control. This includes a summary report on levels of compliance with our information risk policy and whether the policy itself is effective enough.

We ensure the information risk policy is reviewed so that it remains comprehensive and effective at the following intervals and/or after the following events: 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 privacy impact assessments or by consultation with information governance role holders. Risks are documented in an appropriate section of the CAMV corporate risk register which is reviewed at regular intervals by the Trustee Board.

Information risk management

The Senior Information Risk Officer (SIRO) of CAMV 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.

SIRO approval is required before proceeding with any activity likely to generate a significant information risk to CAMV. 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 privacy impact assessment, together with consideration of CAMV's defined risk appetite.

We have adopted the Data privacy impact assessment to perform information risk assessments. Citizens Advice is responsible for information risk assessments for IT systems it provides to store and process client information. We 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.

We 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 Citizens Advice. We report all data security incidents to Citizens Advice as soon as they are detected and where required to the Information Commissioner's Office within 72 hours.

Data handling – through life Information Governance measures

i) Acceptable use
We ensure that all staff and volunteers read and sign our acceptable use policies (AUP), prior to being given access to confidential information, including the AUP for Casebook and 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.

We review our acceptable use policies regularly to ensure they are kept up to date.

ii) Access control

We 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.

We 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.

iii) Data classification

We ensure that all staff and volunteers can easily identify confidential data by clearly labelling the document in the header as 'CONFIDENTIAL'.

iv) Data in transit such as email, fax, or post

We ensure via initial and refresher training that all staff and volunteers understand that CAMV is legally responsible for the security of data sent whilst in transit, including but not limited to data sent via email, webchat, fax, video, mobile applications and post. We ensure that any email containing confidential information is adequately secured by adopting the Citizens Advice recommended secure email procedures. We have adopted the Citizens Advice recommendations on securing faxes to secure our fax transmissions.

v) Retention, deletion and secure disposal

We follow the Citizens Advice retention policy for all client records and other individual records and mark for deletion at the end of the retention period. The record retention periods on an information asset register or retention schedule. We 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

vi) Removable media

We 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.

vii) Personal data in the cloud or externally hosted

CAMV does not routinely store personal data in the cloud or externally.

Where personal data is stored or processed externally a data privacy impact assessment is undertaken and the ICO Cloud Computing guidance is followed. A written 'data processing agreement' must be signed with the supplier.

viii) ICT

We ensure that CAMV implements any necessary IT Security as set out in National Cyber Security Centres 10 steps to Cyber security We use the IT Health check available from Citizens Advice to help us identify and action any improvements that may be required. We ensure that only local Citizens Advice 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 an appropriate local policy. We also ensure that any remote computer processing protected personal data is protected with an identification and authentication mechanism (such as user logon and password). The local Citizens Advice will avoid the use of live or identifiable data in system testing.

ix) Physical security

We protect the physical locations where confidential data is held using a number of layers of security defined in our physical security checklist. We 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.

x) Home working and mobile working

We 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 CAMV Homeworking / outreach policy. See Quality Manual and Staff handbook available in both offices.
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 our staff and volunteer policies.

xi) Assured information sharing

CAMV 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.

xii) Location of personal information

CAMV identifies where all personal data is processed and stored and aims to keep this within the UK or within Europe.
Data processed outside Europe, for example by a US based cloud services provider must refer to how security requirements for this type of transfer are met in a written contract or data processor agreement.

Individual rights

- The right to be informed

We provide appropriate information to our clients across all channels through appropriate privacy notices and just in time notices,

We describe what information is being collected, who is collecting it, how and why is it collected and how it is used and shared. CAMV follows the ICO privacy notice code of practice. We allow members of the public to contact our service by providing clear contact details to exercise their personal data rights such as:

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

CAMV does not use automated decision making or profiling.

Compliance

We ensure that confidential data assets are managed properly by documenting our information assets in an information asset register. We ensure that the data flows of information for that asset are known and documented ensuring data privacy 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.

We employ joining and leaving checklists to ensure that confidential data assets are returned and access to any information is removed when someone leaves CAMV.

We ensure all staff members, volunteers and contractors successfully complete appropriate data protection training and are made aware of the importance CAMV 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 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 office managers. Failure to comply is escalated to the SIRO, and if necessary the Trustee Board, until resolved.
We ensure all our policies are kept up to date to help implement CAMV's effective management of information risks. Our acceptable use policies require all members of staff and volunteers to keep confidential data safe.

All members of staff and volunteers have received training so they know that data security breaches caused by their actions may result in disciplinary or equivalent volunteer proceedings. In some cases this may be considered gross misconduct, and that some instances may be criminal offences under Section 55 of the Data Protection Act 1998 or legislation equivalent to the General Data Protection Regulation. All members of staff and volunteers, including contractors, sign confidentiality or non-disclosure agreements prior to being given access to confidential data.

We regularly review audit information for our main ICT systems to ensure that access to confidential data complies with our acceptable use policies. Any potentially suspicious activity is investigated and remedial actions taken where necessary – which may include retraining or disciplinary proceedings.

We 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.

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

We comply with any mandatory elements of the Citizens Advice 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).

Signed R Rhodes **Date:** 21/3/22

Citizens Advice Mole Valley Trustee Board member