RSPCA Milton Keynes & North Bucks (Reg Charity No: 275415)

Data Governance Policy

v01

Scope

It is a duty of the trustees to ensure that the branch's resources are protected in order that the branch can fulfil its aims. It is important that all those working in the charity whether trustees, staff or volunteers take the issue of data management controls seriously to ensure that information is not put at risk. Making controls work should not be seen as just the responsibility of one or two trustees or senior staff members, or as applying to some but not others.

Data management controls should be just one part of a charity's overall control framework. The wider framework should cover all the branch's systems and activities.

The aims of data management controls are to be clear on:

- How we should handle, review, receive, share or destroy information
- How we should classify information
- How we should store information and how long to retain information
- How we should report a data security incident or loss of device

Overview of information

What is information?

Our information is not limited to, any type of information about our customers, colleagues, volunteers, suppliers or third parties. An example of information we may need to collect:

- Accounts
- Customer, colleague, volunteer, personal details including names, contact numbers, addresses, and bank details
- Sales data from our shops
- Pension details
- Training materials
- Policy documents, procedures, guides and processes
- Performance reviews
- Payslips
- Photographs or images
- Adoption forms

What format could information be in?

Information is kept in many different formats. The most common and obvious ones are listed below, however this is not an exhaustive list, there may be other formats:

- Emails
- Folders or paperwork filed in a cabinet or cupboard or kept on a desk/worktop/counter
- All data and documents stored in computer systems
- Notes taken on a notepad or piece of paper
- Customer, colleague or volunteer letters or complaints
- Post-it notes, notice boards, posters

How to handle information in a safe way

If we don't handle information responsibly, it can be lost or compromised which would put us at risk of fines from governing bodies, it would be brand damaging and it would have an impact on the trust of our customers, colleagues and volunteers.

There are five things to always keep in mind (C.H.A.I.N):

- Confidentiality: making sure the right people have access to information and locations and that unauthorised people don't have access
- Handling: only using information for the purpose it was intended unless you have obtained permission to use it in other ways

- Availability: making sure the right people have access when they need it
- Integrity: making sure information is accurate and up to date
- Necessity: only keep this information for as long as required

Classifying information

Different types of information must be handled appropriately to make sure we meet legal and regulatory requirements and protect our name. locally and nationally. We must identify the level of sensitivity and the harm that might result from its loss or unauthorised disclosure. To do this, we classify information, which will fall into one of three classification categories.

Public

All information which is easily accessible by any member of the public such as a blog on a website, a post on social media or an article in a newspaper. This information can be shared freely with anyone.

Internal

This information is private to our business and we must make sure we don't share it with anyone who doesn't need to know or need to have it e.g. policies, procedures.

Confidential

This information is the most critical information and if it is lost or shared inappropriately could result in major financial, legal, brand or reputational consequences for our branch or National HQ. Confidential information must never be displayed on the wall, noticeboards or anywhere that can be easily seen by many people or visitors and must always be disposed of using a suitable method e.g. cross cut shredders.

Handling payment card information for debit and credit cards

Payment card information for debit and credit cards must be handled with care so we comply with the Payment Card Industry Data Security Standard (PCI DSS).

- Payment cards are any debit, credit, and pre-paid cards branded with one of the five card association/brand logos– American Express, Discover, JCB, MasterCard, and Visa International
- Payment card information is customer information that includes the long number on the front of the card, the expiry date, the information contained in the chip and/or the three- or four-digit security code.
- If the card account number or three- or four-digit security code needs to be written down in full, you must only do so if there's a clear business reason. You must dispose of this immediately and securely after use by shredding it
- Physical copies of payment card information must be stored in locked cabinets and must never be left unattended on desks/counters/work tops or in clear view at any time
- Payment card information must never be stored digitally anywhere on our systems
- Payment card information must never be sent by email, either internally or externally, or by instant messaging, chat or social networking services
- Do not send or store payment card information in a readable format (i.e. the number must be hashed or encrypted).
- Payment card information must never be transferred using public Wi-Fi
- If you need to send payment card information in the mail, make sure contents are secured and use registered post or secure courier so the mail can be tracked to destination
- Payment card information must not be shared with a third party

If payment card information is mishandled or left unprotected it could be lost or stolen. This could mean financial loss to our customers, loss of trust, major damage to our reputation and large fines.

How long should I keep information for? (Data retention)

How long we retain information for will depend on its sensitivity and nature. Below are some guidelines to consider when handling all information:

- **Most importantly you must only keep information if there's a business need to do and for as short a time as possible**
- Only use personal information for the reason it was given to you and never share it with anyone who does not have a business need to know it
- Delete physical and electronic drafts when a document or record is finalised unless there's a business reason e.g. to keep a record of contract changes
- Keep one central version digitally on the shared drive with permissions set to restrict access
- Minimise retention of any paper copies where possible
- If you need to keep a copy and no version exists digitally, you can scan the paper copy and save it as a PDF electronically and then dispose securely of the paper version
- You should regularly review all files on your computer and only keep those where there is a valid business reason to keep them

Employee	Volunteer	Customer	Trustees
• 4 years after the colleague has left the branch	• 1 year after stopping volunteering duties	• 1 year from time of animal adoption	• 4 years
• Any information where there is a regulatory /legal requirement, to keep it beyond 7 years e.g. pay and tax documents, employment contracts			

Loss of information or equipment

Every colleague or volunteer has a responsibility to report the loss of information, devices or security breaches straight away. It's vital that we know about any security breaches immediately so we can take appropriate action and provide guidance.

If there is a loss of documents, USBs, mobile phones, tablets, laptops or other equipment that contains our information or a password or login has been compromised or suspected of, contact the Chair or Secretary immediately or animal co-ordinator. This includes any potential or known security breach too.

Even if you have sent an email with sensitive information to the wrong person, or have clicked on a link in a phishing/suspicious email, we need to know so that we can investigate and reduce the impact it might have on the branch

- If documents or equipment were stolen, you must also report it immediately to the police
- If your account may be compromised, you must change your password as soon as possible
- Depending on the information lost, inform relevant stakeholders

How do I report an incident, security risk or that I've lost information?

You must report any security risks, incidents or loss of information/device/USB/laptop as soon as you're aware to the **MKRSPCA** on **01908 611179** and email **secretary@mkrpsca.org.uk**

Dealing with complaints or queries about how we handle personal data?

Occasionally we receive complaints or queries about how we handle personal data, including requests from individuals for a copy of all the personal data we hold about them (known as data subject rights)

- If you receive a request from any customer, colleague or volunteer for their personal data, please ask them to email **secretary@mkrspca.org.uk**

The branch ICO registration number is: ZA246774

Contact details for The Information Commissioners Office (ICO) can be found at https://ico.org.uk/make-a-complaint/