Information Sheet 4

Data Protection for Village Halls and Community Buildings - A Preliminary Guide

January 2018

acre ACTION WITH COMMUNITIES IN RURAL ENGLAND

Contents

Acknowledgements

This information sheet has been compiled by Louise Beaton, a trustee of ACRE, with reference to material published on the ICO website. Louise is an independent Community Halls Adviser and gratefully acknowledges material shared by the Alliance for the Voluntary Sector.

Introduction

This Information Sheet is a preliminary guide to the regulations as they are most likely to affect Village Halls, Community Centres, Church Halls and similar charitable community buildings. It will be updated as greater clarity about the effect of the regulations emerges.

New data protection legislation comes into effect in May 2018, the General Data Protection Regulations (GDPR).

Village and Community Halls use personal data in a variety of ways. For example:

- Recording information about hirers and trustees
- Circulation lists for newsletters
- Information about tickets for events, fundraising and reclaiming gift aid on donations.

Those responsible for managing your hall (trustees, councillors, committee members, managers and other staff) are defined under the legislation as Data Controllers and therefore need to be aware of how data protection legislation applies to the way in which your hall committee and staff use data.

Before GDPR comes into effect you need to prepare by working out what personal data you hold, review the way you do so and make sure that policies are in place and adhered to.

While large charities raising funds have faced heavy fines for breach of data protection legislation, for most village and community halls the risk of prosecution should be low, providing personal data is:

- held securely, and any breach reported within 72 hours (3 days)
- is only used for the legitimate purpose for which it was collected (such as the examples above) and
- disposed of when no longer required.

The Information Commissioner's Office (ICO) has said that it will be 'proportionate' in its approach to fining charities that break rules when new rules come into force next year: "We will listen to what you have got to say, and what we will be looking for is you to actively be demonstrating that you are working towards some of the issues. If there is a lack of clarity we will demonstrate our understanding of that."

This guidance is not a substitute for legal or professional IT advice. Most village halls are likely to be exempt from the requirement to notify the ICO that personal data is processed. However, parish councils running community buildings may be subject to additional requirements as a result of their local authority functions (for example, a Data Protection Officer has to be appointed).

1 What is Personal Data?

Personal data is any data that relates to an identifiable individual, such as name, address, contact details, age (including trustee dates of birth provided for the Charity Commission's annual return), gender, family details. In addition, of relevance to village halls, it can include:

- Online identifiers e.g. email addresses
- Employee information
- Databases holding contact information e.g. about bookings, newsletter mailings, ticket sales
- CCTV footage
- Financial information
- For fundraising purposes e.g. lists of individual donors, gift aid reclaim records
- For publicity purposes e.g. photos of identifiable people at events.

Certain categories of personal data are subject to strict rules regarding collection and processing, such as racial or ethnic origin, health and medical information and sexual orientation. It is unlikely that many village halls need to hold such data and it is not covered by this Information Sheet.

2 The General Data Protection Regulation - Applying these to your hall

The ICO have prepared a 12-step guide to preparing for the GDPR, which is available on their website. However, not all steps will apply to most village halls so we focus on the 7 key steps below:

2.1 Map the information you hold

You need to work out and document what personal data you hold, where you hold it, where it comes from, who it is shared with and who is responsible for it.

One way of doing this is to:

- Put the item on the agenda for your next committee meeting and ask each trustee and employee to come prepared with information about what personal data they hold, where and who they share it with and
- Record the results (a flip chart may help). Think in terms of paper files, diaries, computers, tablets, phones, memory sticks, CDs, CCTV, archives etc.

Alternatively you could send round a form for committee members to complete.

An example is given in **Appendix A**.

Having mapped the data check that everyone has secure password protection on all their devices and ensure everyone understands the 8 Data Protection principles. These are set out in **Appendix B** and all committee members need to be aware of them.

Check that everyone has secure password protection on all their devices and ensure everyone understands the 8 data protection principles

2.2 Work out the lawful basis for your processing personal data

Personal data must be handled fairly and lawfully. This means that it can be obtained only for lawful purposes and not further processed or shared with others in a manner incompatible with those purposes.

Personal data can lawfully be obtained for the purposes of managing the hall e.g. recording bookings, managing the finances, invoicing, recording trustee information, ticket sales for events etc. You need to minute that this is the lawful purpose for which you hold it.

Personal data obtained for this purpose can be shared in order to facilitate management of the hall. However, data cannot be shared with other organisations unless either for the purposes of managing the hall, or specific consent has been given, or it is in the public domain or an exemption applies, such as with the Police or Social Services in the case of a suspected Child Protection issue.

Personal data obtained for this purpose cannot be used, for example, by individual trustees or employees in connection with their own business unless the individual has given specific consent or the information is in the public domain e.g. by virtue of public advertising of an activity held at the hall.

Trustees, employees and volunteers may find it hard to distinguish between personal data that they hold for their own personal recreational or domestic purposes e.g. membership of a club, family and friends, which is almost totally exempt from regulation, and data obtained by and held for the charity's purposes, which cannot be used other than for the charity's lawful purposes. If they all keep to the habit of ensuring all the personal data they hold is securely held e.g. password protected this should help.

The ICO website has an online self-assessment tool which enables you to check whether you need to register with (notify) the ICO

Most village halls are likely to be exempt from the requirement to notify the ICO that personal data is processed, as exemptions apply for some not-for-profit organisations and for organisations that process personal data only for staff administration, public relations and accounts and records. The ICO website has an online self-assessment tool which enables you to check whether you need to register with (notify) the ICO.

2.3 Check whether you need consent for its use

The GDPR strengthens the requirement to obtain consent from someone to hold their data. While data can be held for the lawful purposes of managing the hall i.e. bookings, staff administration, accounts and records, public relations without specific consent, if it is held or used for other purposes which are incompatible with the original purposes then you will need to obtain consent to use it.

A positive, affirmative action is now needed, which can be a tick box or signed consent form. Every must be captured and filed so that there is full transparency. Consents given before May 2018 must be re-acquired. Consent can be withdrawn at any time.

A positive, affirmative action is now needed, which can be a tick box or signed consent form

An example of a consent form might be:

'Anywhere Village Hall uses personal data for the purposes of managing hall bookings, finances, events and publicity. Please tick here if you are willing for us to share your contact details with other groups and organisations benefitting the residents of the Parish of Anywhere'.

2.4 Review your privacy notices

A village hall may not need to give a privacy notice if it is only processing data for an obvious purpose such as managing the hall's bookings and finances. However, for the avoidance of doubt it can be helpful to provide a privacy notice e.g. on the website, in the hiring agreement so that the purposes for which the charity holds personal data are clear. The period over which data is retained should also be given.

An example of a privacy form might be:

'Anywhere Village Hall uses personal data for the purposes of managing the hall, its bookings and finances, running and marketing events at the hall, staff employment and its fundraising activities. Data may be retained for up to 7 years for accounts purposes and for longer where required by the hall's insurers. If you would like to find out more about how we use your personal data or want to see a copy of information about you that we hold, please contact the hall Secretary'.

2.5 Check your procedures so that they cover all the rights individuals may have

GDPR strengthens the rights of individuals to obtain confirmation from an organisation as to whether or not personal data concerning them is being used, where and for what purpose. A copy of the personal data has to be provided, free of charge unless the request is 'manifestly unfounded

or excessive', in an electronic format, including any emails where they are mentioned. If the data was not obtained from that individual, details of where it came from have to be provided.

This is called a Subject Access Request (SAR). You have 30 days in which to respond and certain information must be provided. However, before providing the information you need to verify the individual's identity otherwise you could commit a data breach.

Individuals also have a number of other rights, of which the two most likely to be relevant to village halls are, the right to have data rectified if incorrect or incomplete and to have data erased where there is no compelling reason for it to continue to be held.

In order to comply with these rights it is important that trustees and employees understand how to deal with them and that there is a policy in place which covers the storage and erasure or destruction of personal data. See section 3.

2.6 Put procedures in place to deal with a data breach

All organisations are required to report certain types of data breach to the ICO and in some cases to the individuals affected. A report to the ICO must be made within 72 hours (3 days) of becoming aware that an incident is reportable.

All organisations are required to report certain types of data breach to the ICO and in some cases to the individuals affected

Ring the ICO's helpline 0303 123 1113 for clarification if you are unsure whether something represents a significant breach.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. You only have to notify the ICO where it is likely to result in a risk to individuals: For example, damage to reputation, financial loss, loss of confidentiality. If a data breach occurs, it is important to check whether anything could be done to avoid it happening again.

The implication for village halls is that all trustees, employees and volunteers need to be aware that it is essential that any PC, laptop, mobile, tablet, CD or memory stick used for village hall purposes is password protected and that if any of these items are stolen or hacked, and risk to individuals results, the breach is reported. The same applies to paper files.

2.7 Consider whether a Data Protection Officer (DPO) needs to be appointed

A parish or town Council running a community building will need to appoint a DPO, because it is a Public Authority. However, it is unlikely that charitable village halls, church halls or community centres or similar organisations will need to appoint a DPO unless handling certain kinds of large scale data.

You can appoint a DPO if you wish to do so. This person could be an employee, trustee, volunteer or an external person. The DPO would need to report to the management committee on the tasks below and s/he would need to have training in or professional knowledge of data protection law, proportionate to the type of processing your hall carries out and the level of protection the personal data requires.

The minimum tasks of a DPO are:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed e.g. employees, customers etc.

3 Next Steps and Practical Issues for Village Halls

Many village hall trustees, volunteers and self-employed people working under contract for village halls use their own personal, or work, computers, tablets, mobiles and other equipment for village hall business. The variety and multiple locations of equipment used make it difficult for a committee of volunteers to control data lawfully used by a village hall, especially when trustees and volunteers retire. Consequently the focus has to be on reducing risk, and particularly risk of data breaches which could result in financial loss or identity theft.

The focus has to be on reducing risk, and particularly risk of data breaches which could result in financial loss or identity theft

Action Point 1:

Insist on password protection for all devices and on internet and malware security.

If any of your trustees, staff or employees have trouble complying with this you may find that providing the services of a knowledgeable student or teenager for a couple of hours will help! Alternatively it would be a wise use of charity resources to recruit the help of a local IT consultant.

Action Point 2:

Consider arrangements for keeping village hall correspondence separate e.g. through the use of a village hall email address such as chair@anywherevillagehall.co.uk. Consider providing employees e.g. a manager or booking secretary with a password protected dedicated mobile phone and/or laptop. This has the advantage that a trustee can take them over while the manager or booking secretary is on holiday.

Action Point 3:

Provide the 8 Data Protection principles to all the hall committee and go through them at a meeting.

Action Point 4:

Prepare (or review) the hall's Privacy Notice and a Consent Form.

Action Point 5:

Prepare policies and procedures.

Action Point 6:

Review your Data Protection policies and procedures regularly.

Adopting some simple policies and procedures will make it easier to communicate what you expect of all your trustees, employees, volunteers and contractors working for you.

A sample policy is given at **Appendix C**. At a minimum your policies should cover:

- Making everyone aware of the risks of identity theft and financial loss if personal data is lost or stolen.
- Requiring password protection and internet security to be installed on all devices handling personal data for the hall, passwords on hall owned equipment and memory sticks with financial records to be stored in an agreed, secure location.
- Setting out how long different kinds of data should be stored for and in what manner. For example, financial records and correspondence to be destroyed after 6 years; employee records to be kept for insurance purposes for up to 40 years, stored securely; duplicate copies of minutes and correspondence destroyed after three years.
- The hall's Privacy Notice and Consent Policy and where consents are stored.
- How to handle a special access request (SAR). The 30 day limit, who else to inform, how to verify their identity e.g. by reference to photo ID and proof of address and providing a link to the ICO website showing the information which has to be supplied.

Requiring password protection and internet security to be installed on all devices handling personal data for the hall, passwords on hall owned equipment and memory sticks

- The need for all personal data acquired on behalf of the hall to be destroyed when no longer needed, when people resign or their contract ends. This means that names, email addresses, telephone numbers will need to be removed from address books unless they also hold that information for personal, domestic or recreational purposes or the individual has provided consent to share it or it is in the public domain. Old paper copies of minutes and correspondence should be shredded if they contain personal data.
- The accident book needs to be checked regularly. A page that has been completed needs to be torn out, appropriate action taken and then filed securely.
- The keeping of archived important documents such as deeds, minute books etc. and historical archive material should be kept securely in a locked filing cabinet in a known location. This might be at the hall, with the Parish Council archives, or at the County Records Office, not in a cardboard box in a shed or garage.

4 CCTV

Use of CCTV is covered both by Data Protection legislation and by the Protection of Freedoms Act (POFA) and the Human Rights Act 1998 and particular care is therefore required in the use, recording, storage and access to recorded material. Separate procedures will be required. This is to ensure that the rights of individuals recorded by surveillance systems are protected and that the information can be used effectively for its intended purpose.

The ICO have published "In the picture: A data protection code of practice for surveillance cameras and personal information", which covers the data protection aspects. A separate code issued under POFA covers issues such as operational requirements, technical standards and systems available.

If your hall has a security issue it is best to discuss with local police first whether it would be appropriate to install CCTV, given the requirements. Another solution such as improved lighting might be cheaper and easier to maintain. Check whether the supplier will provide training in its use so as to enable you to comply with the ICO and POFA codes.

If your hall has a security issue it is best to discuss with local police first whether it would be appropriate to install CCTV

5 How the ACRE Network uses the Personal Data of those running village and community halls

The personal data of those who access ACRE Network services e.g. names, addresses, telephone numbers and email addresses is normally collected only for the ACRE Network's legitimate purposes of providing information and guidance to those running village and community halls. Emails and paper records containing such information are stored as part of membership or subscription schemes, for the distribution of newsletters and information about training and similar events likely to benefit halls, where guidance provided previously is likely to assist in providing guidance again in future (to the same or another hall), or where information contained informs work to tackle issues affecting halls generally.

ACRE Network members make every effort to keep this data up to date. However, when trustees and officers change we are not always informed, which makes it difficult to keep mailing lists up to date. You can help us comply with our own obligations by ensuring your Network member has the current contact information for your hall.

Occasionally we ask for consent to share experience with other halls or carry out research which enables us to monitor changes in the way halls are resourced and used and raise issues with Government. When we do so we make a specific request to use your data and use it only in connection with that work.

Sources of further information and advice

ACRE provides an information and advice service for committees managing halls through the ACRE Network. ACRE publishes a range of village hall publications and information sheets to support the service, which are available from local ACRE Network members. ACRE publications that may be of particular interest to readers of this publication are listed below:

- Information Sheet 17: Trustee roles and responsibilities
- Information Sheet 35: Trustee liability and trustee indemnity insurance
- Information Sheet 37: Fire safety in village halls
- Information Sheet 38: Short guide to security in your village hall

Further Information

Advice for the Voluntary Sector
www.afvs.org.uk
Tel : 0845 319 8330

Louise Beaton
Independent Consultant
Community Halls Advice
www.communityhallsadvice.co.uk
Tel: 01243 544366

Consult the ICO website
www.ico.org.uk

The ICO have launched a helpline for small organisations. Telephone 0303 123 1113 and select option 4 to be diverted to staff who can offer support. A live chat service is also available.

For general information:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

A handy guide to key points and posters

https://ico.org.uk/media/for-organisations/think-privacy/2586/ico-think-privacy-toolkit-charities.pdf

Information about data protection and CCTV

https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

Information about individuals rights of access

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/.

To report a breach online

https://ico.org.uk/for-organisations/report-a-breach/.

Appendix A:
Sample data list or map for a village hall

Example

Chairman	Home pc - names, email addresses and tel numbers for trustees, volunteers and staff. Diary - names and telephone numbers. Mobile – names and telephone numbers.
Secretary	Laptop - dates of birth of trustees (required for Charity Commission return), names, email addresses, tel numbers and addresses for trustees, staff and volunteers, correspondence with hirers and other local people. Diary - names and telephone numbers. Home phone and Mobile – names and telephone numbers. Paper files - records from hall Accident Book. Correspondence with insurers regarding claims and volunteer cover. Hall archives.
Treasurer	Laptop - names, tel numbers, email addresses of trustees; names, email addresses, addresses and bank details of hirers (invoicing & receipts) and employees. Memory Stick – recent financial records. Mobile phone – trustee names and numbers.
Committee members/ trustees	Tablets, PCs, laptops, phones – names, email addresses, tel numbers of trustees, volunteers and friends who help run fundraising events. Photos of people at events.
Staff – Booking Secretary	Laptop – names, telephone numbers, email addresses, addresses of hirers and enquirers. Mobile – names and numbers for trustees and regular hirers.
Volunteers	Gardener – mobile – trustee numbers.
Other	CCTV system – special procedures apply.

Appendix B: The Data Protection Principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Appendix C:
Sample Data Protection Policy

Name of Charity: Anywhere Village Hall (AVH)

Data Protection Policy and Procedures

Introduction

We are committed to a policy of protecting the rights and privacy of individuals. We need to collect and use certain types of Data in order to carry on our work of managing Anywhere Village Hall (AVH). This personal information must be collected and handled securely.

The Data Protection Act 1998 (DPA) and General Data Protection Regulations (GDPR) govern the use of information about people (personal data). Personal data can be held on computers, laptops and mobile devices, or in a manual file, and includes email, minutes of meetings, and photographs.

The charity will remain the data controller for the information held. The trustees, staff and volunteers are personally responsible for processing and using personal information in accordance with the Data Protection Act and GDPR. Trustees, staff and volunteers who have access to personal information will therefore be expected to read and comply with this policy.

Purpose

The purpose of this policy is to set out the AVH commitment and procedures for protecting personal data. Trustees regard the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal with. We recognise the risks to individuals of identity theft and financial loss if personal data is lost or stolen.

The following are definitions of the terms used:

Data Controller - the trustees who collectively decide what personal information AVH will hold and how it will be held or used.

Act means the Data Protection Act 1998 and General Data Protection Regulations - the legislation that requires responsible behaviour by those using personal information.

Data Protection Officer – the person responsible for ensuring that AVH follows its data protection policy and complies with the Act. [AVH is not required to appoint a DPO].

Data Subject – the individual whose personal information is being held or processed by [AVH] for example a donor or hirer.

'Explicit' consent – is a freely given, specific agreement by a Data Subject to the processing of personal information about her/him.

Explicit consent is needed for processing "sensitive data", which includes:

(a) Racial or ethnic origin of the data subject
(b) Political opinions
(c) Religious beliefs or other beliefs of a similar nature
(d) Trade union membership
(e) Physical or mental health or condition
(f) Sexual orientation
(g) Criminal record
(h) Proceedings for any offence committed or alleged to have been committed

Information Commissioner's Office (ICO) - the ICO is responsible for implementing and overseeing the Data Protection Act 1998.

Processing – means collecting, amending, handling, storing or disclosing personal information.

Personal Information – information about living individuals that enables them to be identified – e.g. names, addresses, telephone numbers and email addresses. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers.

The Data Protection Act

This contains 8 principles for processing personal data with which we must comply.

Personal data:

1. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,

2. Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,

3. Shall be adequate, relevant and not excessive in relation to those purpose(s).

4. Shall be accurate and, where necessary, kept up to date,

5. Shall not be kept for longer than is necessary,

6. Shall be processed in accordance with the rights of data subjects under the Act,

7. Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,

8. Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

Applying the Data Protection Act within the charity

We will let people know why we are collecting their data, which is for the purpose of managing [the hall], its hirings and finances. It is our responsibility to ensure the data is only used for this purpose. Access to personal information will be limited to trustees, staff and volunteers.

Correcting data

Individuals have a right to make a Subject Access Request (SAR) to find out whether the charity holds their personal data, where, what it is used for and to have data corrected if it is wrong, to prevent use which is causing them damage or distress, or to stop marketing information being sent to them. Any SAR must be dealt with within 30 days. Steps must first be taken to confirm the identity of the individual before providing information, requiring both photo identification e.g. passport and confirmation of address e.g. recent utility bill, bank or credit card statement.

Responsibilities

[AVH] is the Data Controller under the Act, and is legally responsible for complying with Act, which means that it determines what purposes personal information held will be used for.

The management committee will take into account legal requirements and ensure that it is properly implemented, and will through appropriate management, strict application of criteria and controls:

a) Collection and use information fairly.

b) Specify the purposes for which information is used.

c) Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements.

d) Ensure the quality of information used.

e) Ensure the rights of people about whom information is held, can be exercised under the Act.

These include:

i) The right to be informed that processing is undertaken.

ii) The right of access to one's personal information.

iii) The right to prevent processing in certain circumstances, and

iv) the right to correct, rectify, block or erase information which is regarded as wrong information.

f) Take appropriate technical and organisational security measures to safeguard personal information,

g) Ensure that personal information is not transferred abroad without suitable safeguards,

h) Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information,

i) Set out clear procedures for responding to requests for information.

All trustees, staff and volunteers are aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them.

[If appointed]: The Data Protection Officer on the management committee is:

Name:

Contact Details:

The Data Protection Officer will be responsible for ensuring that the policy is implemented and will have overall responsibility for:

a) Everyone processing personal information understands that they are contractually responsible for following good data protection practice

b) Everyone processing personal information is appropriately trained to do so

c) Everyone processing personal information is appropriately supervised

d) Anybody wanting to make enquiries about handling personal information knows what to do

e) Dealing promptly and courteously with any enquiries about handling personal information

f) Describe clearly how the charity handles personal information

g) Will regularly review and audit the ways it holds, manages and uses personal information

h) Will regularly assess and evaluate its methods and performance in relation to handling personal information.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998.

In case of any queries or questions in relation to this policy please contact [the Data Protection Officer].

Procedures for Handling Data & Data Security

[AVH] has a duty to ensure that appropriate technical and organisational measures and training are taken to prevent:

- Unauthorised or unlawful processing of personal data
- Unauthorised disclosure of personal data
- Accidental loss of personal data

All trustees, staff and volunteers must therefore ensure that personal data is dealt with properly no matter how it is collected, recorded or used. This applies whether or not the information is held on paper, in a computer or recorded by some other means e.g. tablet or mobile phone.

Personal data relates to data of living individuals who can be identified from that data and use of that data could cause an individual damage or distress. This does not mean that mentioning someone's name in a document comprises personal data; however, combining various data elements such as a person's name and salary or religious beliefs etc. would be classed as personal data, and falls within the scope of the DPA. It is therefore important that all staff consider any information (which is not otherwise in the public domain) that can be used to identify an individual as personal data and observe the guidance given below.

Privacy Notice and Consent Policy

The private notice and consent policy are as follows:

Consent forms will be stored by the Secretary in a securely held electronic or paper file.

Operational Guidance

Email:

All trustees, staff and volunteers should consider whether an email (both incoming and outgoing) will need to be kept as an official record. If the email needs to be retained it should be saved into the appropriate folder or printed and stored securely.

Remember, emails that contain personal information no longer required for operational use, should be deleted from the personal mailbox and any "deleted items" box.

Phone Calls:

Phone calls can lead to unauthorised use or disclosure of personal information and the following precautions should be taken:

- Personal information should not be given out over the telephone unless you have no doubts as to the caller's identity and the information requested is innocuous.
- If you have any doubts, ask the caller to put their enquiry in writing.
- If you receive a phone call asking for personal information to be checked or confirmed be aware that the call may come from someone impersonating someone with a right of access.

Laptops and Portable Devices:

All laptops and portable devices that hold data containing personal information must be protected with a suitable encryption program (password).

Ensure your laptop is locked (password protected) when left unattended, even for short periods of time.

When travelling in a car, make sure the laptop is out of sight, preferably in the boot.

If you have to leave your laptop in an unattended vehicle at any time, put it in the boot and ensure all doors are locked and any alarm set.

Never leave laptops or portable devices in your vehicle overnight.

Do not leave laptops or portable devices unattended in restaurants or bars, or any other venue.

When travelling on public transport, keep it with you at all times, do not leave it in luggage racks or even on the floor alongside you.

Data Security and Storage:

Store as little personal data as possible on your computer or laptop; only keep those files that are essential. Personal data received on disk or memory stick should be saved to the relevant file on the server or laptop. The disk or memory stick should then be securely returned (if applicable), safely stored or wiped and securely disposed of.

Always lock (password protect) your computer or laptop when left unattended.

Passwords:

Do not use passwords that are easy to guess. All your passwords should contain both upper and lower-case letters and preferably contain some numbers. Ideally passwords should be 6 characters or more in length.

Protect Your Password:

- Common sense rules for passwords are: do not give out your password
- Do not write your password somewhere on your laptop
- Do not keep it written on something stored in the laptop case.

Data Storage:

Personal data will be stored securely and will only be accessible to authorised volunteers or staff.

Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately. For financial records this will be up to 7 years. For employee records see below. Archival material such as minutes and legal documents will be stored indefinitely. Other correspondence and emails will be disposed of when no longer required or when trustees, staff or volunteers retire.

All personal data held for the organisation must be non-recoverable from any computer which has been passed on/sold to a third party.

Information Regarding Employees or Former Employees:

Information regarding an employee or a former employee, will be kept indefinitely. If something occurs years later it might be necessary to refer back to a job application or other document to check what was disclosed earlier, in order that trustees comply with their obligations e.g. regarding employment law, taxation, pensions or insurance.

Accident Book:

This will be checked regularly. Any page which has been completed will be removed, appropriate action taken and the page filed securely.

Data Subject Access Requests:

We may occasionally need to share data with other agencies such as the local authority, funding bodies and other voluntary agencies in circumstances which are not in furtherance of the management of the charity. The circumstances where the law allows the charity to disclose data (including sensitive data) without the data subject's consent are:

a) Carrying out a legal duty or as authorised by the Secretary of State Protecting vital interests of a Data Subject or other person e..g. child protection

b) The Data Subject has already made the information public

c) Conducting any legal proceedings, obtaining legal advice or defending any legal rights

d) Monitoring for equal opportunities purposes – i.e. race, disability or religion

We regard the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

We intend to ensure that personal information is treated lawfully and correctly.

Risk Management:

The consequences of breaching Data Protection can cause harm or distress to service users if their information is released to inappropriate people, or they could be denied a service to which they are entitled. Trustees, staff and volunteers should be aware that they can be personally liable if they use customers' personal data inappropriately. This policy is designed to minimise the risks and to ensure that the reputation of the charity is not damaged through inappropriate or unauthorised access and sharing.