Data Protection Checklist

It is a requirement of the 1998 Data Protection Act that anyone storing personal data (information that can identify a living person) must store that data in accordance with the eight principles of Data Protection. Information about these principles can be found here; http://www.ico.gov.uk/for_organisations/data_protection/the_guide.aspx

Not every organisation that holds personal data will require to register with the Information Commissioner but all personal data must be stored in a confidential and secure manner. To find out if you need to register go to the Information Commissioner's website at www.ico.gov.uk

Be aware that a number of unscrupulous organisations may contact you demanding large payments to "register for Data Protection".
If in doubt check the Information Commissioners website at www.ico.gov.uk

Helpline: 0303 123 1113 (local rate) Monday – Friday 9 -5pm.

Data Protection Laws will be changing as of 2018 see: http://www2.cipd.co.uk/pm/peoplemanagement/b/weblog/archive/2017/03/27/get-ready-for-2018-s-changes-to-data-protection-laws.aspx

It is obviously important to keep any personal information collected confidential and secure. This information is only seen by personnel on a 'Need to Know' basis. Trustees do not need to see volunteers personnel files just because they are a Trustee. It is important to know when and how to share personal information and with who.

The following checklist can help you to develop policy which complies with regulation:

Checklist	**Do You Have**	**Tick When In Place**
Store only what is essential and accurate information.		
Secure storage for all confidential information. Ie in a locked filing cabinet		
Written permission to pass confidential information about a volunteer on to other people, within or out with the organisation, must be obtained from the volunteer.		
Access to confidential information restricted to those with a genuine need to know.		
Information you gather about an individual that is no longer required should be destroyed by shredding, e.g. selection documents, DBS information.		
Only obtain references for those volunteers who you intend to accept as volunteers.		

This right, commonly referred to as subject access, is created by section 7 of the Data Protection Act. It is most often used by individuals who want to see a copy of the information an organisation holds about them. However, the right of access goes further than this and an individual who makes a written request (there could be a possible fee incurred to the Individual, Please see guidance listed below) is entitled to be:

- told whether any personal data is being processed
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people; given a copy of the information comprising the data and given details of the source of the data (where this is available).

In most cases you must respond to a subject access request promptly and in any event within 40 calendar days of receiving it. However, some types of personal data are exempt from the right of subject access and so cannot be obtained by making a subject access request. For more information, please see https://ico.org.uk/for-organisations/guide-to-data-protection/exemptions/

For a subject access request to be valid, it should be made in writing. You should also note a request sent by email or fax is as valid as one sent in hard copy.

An organisation receiving a subject access request may charge a fee for dealing with it, except in certain circumstances relating to health records. If you choose to charge a fee, you need not comply with the request until you have received the fee. The usual maximum fee you can charge is £10. There are different fee arrangements for organisations that hold credit, health or education records. Please see the subject access code of practice for more information https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf

The Act allows you to confirm two things before you are obliged to respond to a request.

You can ask for enough information to judge whether the person making the request is the individual to whom the personal data relates. This is to avoid personal data about one individual being sent to another, accidentally or as a result of deception.

The key point is that you must be reasonable about what you ask for. You should not request lots more information if the identity of the person making the request is obvious to you.

You are also entitled before responding to a subject access request to ask for information that you reasonably need to find the personal data covered by the request. Again, you need not comply with the subject access request until you have received this information. In some cases, personal data may be difficult to retrieve and collate. However, it is not acceptable for you to delay responding to a subject access request unless you reasonably require more information to help you find the data in question.

Please see https://ico.org.uk/media/for-organisations/documents/1599/subject-access-checklist.pdf for how to handle a subject access request.