BRITISH PSYCHOTHERAPY FOUNDATION

Registered charity number 115080

handling trainee & post qualification personal data

introduction

The Data Protection Act 1998 and the Freedom of Information Act 2000 are the two pieces of legislation governing access to information about individuals held by the ***bpf***. The Data Protection Act is concerned with personal information about an individual, for example, name, address and date of birth, and has clear rules for the handling of personal data. The Data Protection Act also gives rights to an individual about whom personal information is processed or held.

The Freedom of Information Act provides a general right of access, subject to certain prescribed exemptions, to all information such as policies and procedures, committee minutes and papers.

All members of staff and ***bpf*** members involved in delivering qualification and post qualification training who handle personal information (in this case specifically trainee or post qualification information) must not only comply with the requirements of the Data Protection Act 1998 and the Freedom of Information Act 2000 but will be expected to understand that the need for confidentiality extends beyond the requirements of the Acts, particularly where sensitive personal information is concerned.

This policy has been developed to support the ***bpf***'s Data Protection Policy and the ***bpf***'s commitment to protecting the privacy and confidentiality of the data for trainees and ***bpf*** members undertaking post qualification courses as far as is reasonably practicable.

collection & management of data

Personal information is collected by the ***bpf*** for a number of purposes, both internal to the organization and for external qualification and registration bodies. Staff and members of training committees have a duty to ensure that the information collected is for the stated purpose, that it is factual, and that information is kept securely and destroyed in accordance with ***bpf***'s polices and statutory regulations.

The ***bpf*** needs to hold personal information about trainees and ***bpf*** members for various teaching, qualification, post qualification, CPD and administrative purposes in order to effectively administer an individual's clinician and academic career including:

- maintaining trainee records (including personal, clinical and academic details) and managing processes (for example, awarding of pre training and post training qualifications).
- providing advice to trainees
- accessing facilities such as the library and PEPWEB
- monitoring quality and performance

Information is held in a number of different formats and various locations.

duties of staff & training committees

All those who have access to data as part of their roles should at all times ensure that:

- data are only used for the purpose(s) for which they were collected;
- data confidentiality is maintained at all times;
- data accuracy is maintained;
- data are held securely (see section on security of data);
- only data that are necessary are retained;
- confidential data, whether held in paper format or electronically, are securely destroyed when no longer required.

In addition, all those handling data should be aware of a trainee's right to privacy in matters relating to his/her health and welfare. Under the Human Rights Act 1998, Article 8, states, "Everyone has the right to respect for private and family life, his home and his correspondence".

Anyone who discloses personal data without proper authorization may be subject to disciplinary action.

information to be recorded

The contents of all files, whether paper or electronic files, should be limited to documents that relating to ***bpf***'s professional activities. The documents held should have either been copied to the trainee or member or could be copied without causing any distress. All information recorded should be factual. Judgments, comments or opinions should not be included unless information exists to support those judgments or opinions.

security of data

Personal data should be stored securely. Personal data should be:

- kept in a locked filing cabinet, drawer, or room, whether it is in paper or electronic format when not being worked on or when the room is left unattended (even for a short time).
- not be visible, either on desks or on computer screens, to any visitors (screen savers and computer screen locks used be used). Passwords should not be disclosed to anyone.
- passed in a sealed envelope, if transferred within the organization
- not sent via email, if it is sensitive information
- not disclosed orally or in writing without the permission of the trainee unless it is part of a legitimate ***bpf*** process
- not left on shared printers/ photocopiers
- disposed of securely

If as a member of a Training or Post Qualification Committee you are individually collecting personal data for your own use e.g. by compiling a spreadsheet or database of your own group of trainees; creating a list of seminar leaders or trainees with contact details, or other personal information about them, in order to fulfil your own role, then you need to ensure that you do the following:

- Keep the data securely: safe from unauthorized access, and safe from damage or loss
- Make sure that it is up-to-date and accurate
- Make sure that you only keep it as long as necessary and dispose of it securely.

sharing information

Information can be shared within the ***bpf*** but it should not be shared freely. There should be a good reason for the information to be shared, and the minimum amount of information should be shared each time. It is particularly important to make sure that information about sensitive issues, including disability, sexuality or ethnicity, is not shared unless it is necessary.

If you pass information through e-mail or internal post you need to make sure that it will safely reach the person you mean to send it to, and won't accidentally be seen by anyone else. This means checking the name in the e-mail "to" box carefully before hitting "send" or writing the name clearly on an envelope. Envelopes and e-mails should be marked "confidential". You should avoid faxing personal information as this isn't secure or confidential.

working outside of *bpf* premises

If you are carrying out work away from *bpf* premises, e.g. home, you still have to abide by the Data Protection Act. It is important that no personal information is accidentally lost or revealed to anyone who doesn't have a right to see it.

It is preferable to put records and information somewhere that can be accessed from your home without having to be physically carried there in paper form or on a USB.
Consider finding a way to anonymise information that you need, encrypt it or password protect it (see *bpf* how to password protect guidelines).

If you work on electronic information at home make sure you do not save it to your own computer. If you need to do that while you are working on it then remember to delete it when you have finished. If you need to print something out when you are at home you should either shred it afterwards (if you are able) or bring it back to the *bpf* premises for shredding.

A system for recording who has taken information away, what information they took, when they took it, why they took it, and when they bring it back again should be put in place.

Information (e.g. application forms and interviews notes) should be returned to the appropriate *bpf* premises for secure storage when they are no longer required.

retention and disposal

Trainee data will be destroyed or deleted seven years after qualification. However, some trainee personal information will be retained indefinitely as part of the *bpf*'s membership records and to enable the *bpf* to provide proof of a trainee's achievement.

At the end of a designated retention period, appropriate action should be taken to delete records. Records should be disposed of using an appropriate method. This may be deleting for electronic records, or disposing of in the appropriate waste-bin for non-confidential records.

All confidential records, including those containing personal information should be disposed of by shredding.

APPENDIX 1

how to password protect your work for pc & mac

IF YOU HAVE A PC

Set a password in a Word 2007

- To encrypt your file and set a password to open it:
- Click the **Microsoft Office Button,** point to **Prepare**, and then click **Encrypt Document**.
- In the **Encrypt Document** dialog box, in the **Password** box, type a password, and then click **OK**.
- You can type up to 255 characters. By default, this feature uses AES 128-bit advanced encryption. Encryption is a standard method used to help make your file more secure.
- In the **Confirm Password** dialog box, in the **Re-enter password** box, type the password again, and then click **OK**.
- To save the password, save the file.

Set a password in a Word 2010 & 2013

- Go to file
- Permissions, Protect Document
- Encrypt with password

IF YOU HAVE A MAC

- Click the Word menu
- Select **Preferences**
- Click **Security** in the left side of the dialog box
- Enter a password in the box labelled "**password to open**"
- Click OK
- Re-enter the password when prompted
- Click OK

You can also set a password to modify the document:

- In the security section, type a password in the box labelled "**password to modify**"
- Click OK
- Re-enter the password when prompted
- Click OK