BPP Privacy Policy

Any user of the Best Practice People Limited website accepts unreservedly, by using the site, the terms and conditions for its use that are set out here.

These terms include the legal jurisdiction within which any legal issues arising from the operation of the site may be addressed. Any person who does not wish to accept these terms and conditions or who knows, or ought to know, of any reason why these terms and conditions might not be capable of applying to their purposes, is not authorised to use this site. These terms apply to each and every visit that a user may make to this site.

Purposes and Disclosures
Depending on the preferences indicated by you, we may use your personal data to contact you about your development.

We may disclose your information to third parties who may take over some or all of the Best Practice People business in the future.
If you enrol in a Best Practice People centre we will disclose your personal data to the approved service provider that will be delivering and supporting you. Following registration and enrolment, with a Best Practice People employee, all of our approved service providers will have access to your name, date of birth, address, telephone number, email address and Best Practice People reference number.

Your Choices
You always have the right to view the personal information we keep about you. You can request an overview of your personal data by emailing us on grant@bestpp.co.uk. Please write 'Request personal information' in the subject line of your email to speed things along a bit.

You can also contact us if you believe that the personal information we have for you is incorrect, if you believe that we are no longer entitled to use your personal data, or if you have any other questions about how your personal information is used or about this Privacy Statement. Please email, grant@bestpp.co.uk or write to us at *Grant Basson, CEO, Best Practice People, Pinnacle House, Station Way, Crawley. West Sussex. RH10 1JH.* We will handle your request in accordance with the General Data Protection Regulation.

Important Information
Your personal data is protected by UK data protection law. You can find the details for the UK Information Commissioner at https://ico.org.uk

Data Retention
Best Practice People only retains data, both physical and electronic, for as long as required. This is determined by using Best Practice People's Document Retention policy.
All data held where the retention period has expired will;

- Electronically – be deleted, including backups, and where necessary hard drives shredded by a certified method in the presence of Best Practice People's Data Security Manager.
- Hard copies – be shredded by a certified company in the presence of Best Practice People Data Security Manager.

This policy will be reviewed every 12 months by Best Practice People Limited. Last Update: 1st March 2022

Our Commitment to Privacy
All individuals who have access to Best Practice People records, files or confidential information are required to maintain confidentiality. This statement relates to all staff, volunteers and individuals on work experience or contractors. It may, where necessary, also include those individuals who Best Practice People may work in partnership with, where sharing information is imperative to the needs of the individual. To acknowledge the requirements of the policy all individuals noted above will be expected to sign a confidentiality statement. All individuals noted above will be expected to abide by the requirements of this policy. Copies of the policy will be made available to any external agency that so requests it.

Staff, volunteers (including individuals on work experience) and contractors should note the confidential nature of contact details of our funders, partners, participants and employers and use of these details outside of work undertaken for Best Practice People would be considered a serious breach of confidentiality. Such a breach may result in disciplinary action, which could include termination of employment and / or legal action. Staff, volunteer's individuals on work experience or contractors who have ceased working with Best Practice People should note that they also have a contractual obligation to abide by this statement. Failure to do so may result in legal action being exercised.

Access to Records
Only authorised staff have access to participant's records. Such records will be kept secure in locked cabinets at Best Practice People offices. Keys must be deposited and maintained in the designated place to prevent accidental breaches of confidentiality. Information on computer will be accessed via the appropriate staff member's password. Where the Senior Management require access to participant records a formal request should be made.
We will advise the participant that we are maintaining confidential records concerning them and advise them of our confidentiality policy and their right to access their file if they so request it (Subject Access Request). Access to files by participants should be provided on an appointment basis and viewings will be accompanied by a Best Practice People member of staff.

No file may be taken out of Best Practice People buildings, unless they are required for use at an offsite meeting with a participant, in which case, files would be tracked using 'File Tracker' records.
All letters must be typed, the word processor / operator who produces these documents will abide by the confidentiality policy and procedures. General typing or reports should refer to the individual by reference number.
All superfluous information should be shredded.
All relevant aspects of the Data Protection Act and GDPR must be adhered to.
Where highly confidential information is obtained this should be maintained in an envelope marked 'CONFIDENTIAL' within an individual's file. Within computer records this should be accessible by password only, whereby the password is known only to authorised staff.
Details displayed within the Best Practice People office should relate to an individual by reference number only.
Information from participant files may be used as case study examples for the purposes of:-

- Providing examples during training to internal staff and external organisations;
- Providing case study examples for accredited training evidence portfolios;

All information used for the above circumstances should be anonymised using first names or initials only. Personal contact information must be deleted from such information prior to use.

Finance Records
These records are only accessible to authorised staff, Senior Management and authorised contractors. It is advisable that computer records are accessible by password and that all 'hard copy' information is maintained in a locked cupboard or drawer.

All finance records which relate to personal staff information e.g. wages, payments etc. are considered highly confidential and should be maintained by either the Finance Manager, CEO or the COO. Where other staff accidentally access this information they are required to abide by this policy. Disclosure of personal financial information will be considered serious breach of confidentiality.

It is advisable that all finance records are maintained at Best Practice People's Head office with back up produced in relation to computerised information. These would be maintained appropriately.

Photocopying or typing of finance records should be produced by authorised staff only.
All superfluous information or information that has expired should be archived or shredded to maintain confidentiality.

All relevant aspects of the General Data Protection Regulation must be adhered to.

Personnel Records
All personnel records must be maintained within a locked drawer, where access is controlled by either the Line Manager, Assistant to CEO or CEO. Likewise, computerised records should only be accessible via a password. Disclosure statements from the Disclosure Barring Service will be maintained separately from an individual's personnel records, within Best Practice People's fireproof, lockable unit. Such records will be destroyed within 6 months in line with the regulations. No copies of such information will be made for retention at other sites.

Staff will be able to access and review their personal file twice per annum following a request to their line manager and viewings will be accompanied by a Best Practice People manager. Where a staff member requests to view their personal file in addition to this the file should be accessed via their line manager or the CEO.

Where a Senior Manager requires access to a particular staff member's file a request should be made to the CEO stating the purpose. Authorisation will be provided in conjunction with clarification from Best Practice People's Data Security Manager.

Where a representative of the staff member e.g. Union Representative requests the access to the individual's file written authorisation must be provided by the staff member concerned.
Photocopying or typing of personnel records should be produced by authorised staff only.
Completion of personnel forms should be produced by authorised staff only.
All superfluous or expired information should either be archived or shredded to maintain confidentiality
All relevant aspects of the General Data Protection Regulations must be adhered to.
Best Practice People is not at liberty to divulge telephone numbers or addresses of personnel to a third party, but will pass on numbers or addresses of the third party to the individual concerned.

Telephones
No information concerning a Best Practice People participant may be discussed over the telephone unless that person is known to you and is a person who is accredited with having a genuine need to know.

Exceptions to Confidentiality
The following should be authorised by a member of Senior Management at Best Practice People e.g. CEO, COO, Line Manager, Quality & Compliance Manager or Data Security Manager.

- Risk to the participant's own life, e.g. mental health crisis.

- Serious danger to other people e.g. child abuse.
- Legal requirements to provide or exchange information e.g. juvenile court.
- Where it is anticipated that a serious criminal offence is being committed.
- Where a Best Practice People participant is missing and s/he is considered to be in danger, the local police may be contacted.
- When cooperation in planning services for participants necessitates the exchange of personal information, e.g. Benefit Agency, Doctor, Employer.

Cookies

When you enter our site your computer will automatically be issued with a cookie. Cookies are devices that identify your computer to our server and personalise the site for your future use. Cookies only record the areas of our site that a computer has visited. A cookie will not provide us with any personal information. Therefore, if you have not supplied us with any personal information, you can still browse our site anonymously. If you do not want a cookie you can set your browser to deny it.