Bristol Older People's Forum CIO
Canningford House, 38 Victoria Street, Bristol, BS1 6BY
bopfadmin@ageukbristol.org.uk, 0117 927 9222
www.bopf.org.uk

Bristol Older People's Forum
Confidentiality Policy

Introduction

Bristol Older People's Forum (BOPF) is committed to the principles of confidentiality and believes that they must be integrated across all of our activities. We believe our members, employees and service users deserve the right to confidentiality to protect their interests and to safeguard our own actions.

When circumstances require it, BOPF will offer a confidential service. Nothing told to us in these circumstances will be shared with any other organisation or individual without the express permission of the person(s) concerned unless it is necessary to protect the safety of that individual or another person.

BOPF will ensure that all statistical data and records provided to third parties shall be produced in anonymous form so that individuals cannot be recognised.

BOPF will ensure that all individual's records are kept in a locked, secure place.

Definition

Confidentiality means that no information regarding a member, employee or service user shall be given directly or indirectly to any third party outside the organisation without that person's express consent (if possible in writing) to disclose such information. No discussion of an individual member, employee or service user should take place outside of BOPF meetings.

Legislative Background

Common Law. Personal information about children under 18, families and vulnerable adults held by professionals and agencies is subject to a legal duty of confidence and should not normally be disclosed without the consent of the subject. However, the law permits the disclosure of confidential information necessary to safeguard children and vulnerable adults.

Data Protection Acts 1996/1998. These require that personal information is obtained and processed fairly and lawfully, only disclosed in appropriate circumstances, is accurate, relevant and not held longer than necessary, and is kept securely. They allow for disclosure without the consent of the subject under certain conditions. The Data Protection Registrar has produced a checklist for setting up information sharing arrangements.

Human Rights Act 1998. Disclosure of information without consent might give rise to a challenge under Article (8). However, disclosure of information to safeguard vulnerable people would be justifiable for the protection of "health and morals", for the protection

of the "rights and freedom of others" and for the prevention of disorder or crime. Disclosure should be appropriate for the purpose and only to the extent necessary to achieve that purpose. This is called proportionality.

Public Disclosure Interest Act 1999. This is the "Whistle-blowing Act", which gives protection to employees and others to breach their duty of confidentiality to their employer where the employee has a reasonable belief that it is in the public interest to 'blow the whistle' outside the organisation to disclose malpractice. Examples include where a criminal offence has or is likely to be committed, a legal obligation is not being met, health and safety may be endangered, or there is a concealment of information in connection with the alleged malpractice.

The Caldicott Principles 1997. These are that information sharing:

- justifies the purpose for the transferring of information
- only uses what information is necessary
- uses the minimum information that is required
- access is on a strict need to know basis (defined by the organisation concerned)
- ensures all staff, trustees, volunteers, members etc are aware of their responsibilities, and that they understand and comply with the law.

Other Legislation and Protocols. Include the Access to Personal Files Regulations 1989, BCC policies for the protection of vulnerable adults and children ("No Secrets in Bristol" and "Working Together"), Connexions West of England code of practice for information sharing, Avon and Wiltshire local health and social care communities protocol for sharing information about mental health service users, and protocols for sharing information between agencies in Avon health communities.

Sharing Information

All members and employees have an obligation to safeguard the confidentiality of personal information, subject to the needs of safeguarding children and vulnerable adults. This is governed by law, by contract of employment, and for some by professional codes of conduct.

Breach of confidentiality is a disciplinary matter and can be a criminal offence. It will be dealt with through the BOPF Disciplinary Procedure whether the allegations have arisen through a formal or informal complaint or a potential breach has come to the management committee's attention in some other way.

Individuals must be give consent if information about them may be to be passed on for a relevant purpose and they must be informed if it is to be passed on for safeguarding reasons.

Where there is a risk to the safety and wellbeing of an individual or society, information may be shared even where permission has <u>not</u> been given. If a vulnerable adult's safety or wellbeing is in question the Management Committee of Forum Manager will follow

procedures as set out in Bristol City Council's No Secrets In Bristol guidelines, a copy of the guidelines will be provided to all Management Staff and the Forum Manager.

The Data Protection Act 2018

(This is the UK's implementation of the General Data Protection Regulation (GDPR)).

Under this Act everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

member of staff

In all but defined cases (e.g. disciplinary procedures), the ultimate reference point for deciding who should be informed of a piece of confidential information is the individual to whom it applies. It is important, however, that where consent is given that it is informed consent. For this to be the case it is necessary to tell the person concerned why there is a need to disclose information and to whom. The person should also be told of the likely consequences of their agreeing or not agreeing to this. Once consent has been obtained, it is the responsibility of the person passing on any information to ensure that this is only done on the terms agreed.

Disclosure of confidential information may require written authorisation by the individual concerned. This should be dated and specify to whom disclosure is authorised. A request for an employee's home address and telephone number should always be referred to the

individual concerned before any information is disclosed. This is done via the line manager. There are some agencies who have some automatic right of access to certain parts of personnel information e.g. Inland Revenue or tax queries. Staff should never divulge a colleague's personal circumstances, including their address, future work place etc to anyone without permission of the worker.

Record Keeping

This procedure covers all records held by BOPF concerning staff, volunteers and service users.

Personnel Records

- All staff will be given a copy of the confidentiality procedure as part of their induction. The implications of the procedure for their work will be explained.
- Access to personnel files can be arranged with the line manager who should make clear the following:
    - who has access to files and the procedure for gaining access
    - how the information is stored, e.g. locked cabinet
- Application forms, interview records, medical information and monitoring forms are confidential to BOPF.
- Equal opportunity monitoring forms will be detached from application forms on receipt and kept separate from application forms.
- References - when seeking references for a new employee it is made clear to the referees that information is sought in confidence.
- Probationary reviews and appraisals. The line manager should make clear who receives information on the review.
- Medical records will be held on personnel files in a sealed envelope. Copies of medical certificates and self certification forms will be placed on personnel files after action for payroll purposes.
- Breaches of confidentiality by staff will normally be treated within the remit of BOPF's disciplinary and grievance procedure. The nature of any breaches of this procedure will determine the level of disciplinary action, e.g. disclosure of unauthorised staff details would be gross misconduct.

Service users

Any paper information should be kept in a filing cabinet, which is kept locked. All files must be returned to the cabinet after use.
All service users are protected under the Data Protection Act 1998.
Service users are expected to respect the rights of other service users to confidentiality and privacy particularly as regards personal information known about another service user.

Partnerships with other organisations

BOPF may be working in partnership with other bodies. Where specific information-sharing protocols exist that affect a particular service user all agencies should be aware of this.

BOPF will give all partnership agencies a copy of the confidentiality procedure and will explain the requirements it places on the partnership organisations.
It will be agreed at the outset which staff in the partner organisation will have access to information and in what circumstances.
Management agreements will state that breaches of confidentiality by either party will be treated as a breach of the agreement

IMPLEMENTATION
Date implemented: June 2012, **Next review date: October 2025**

REVIEW OR AMENDMENTS TO POLICY
Reviewed by Pat Foster, BOPF Trustee **Date reviewed: October 2023**
Date adopted at Trustee Meeting: 19 October 2023

Signed: Christina Stokes, BOPF Chair, 19 October 2023

Bristol Older People's Forum CIO is registered in England and Wales
Registered Office: Canningford House, 38 Victoria Street, Bristol, BS1 6BY
Registered Charity Number: 1162616