Confidentiality and Data Protection Policy

Adopted by MT June 2017

Table of Contents

Section 1: Introduction

Data (information and knowledge) is essential to all aspects of the work of Ballyfermot Chapelizod Partnership (BCP). In collecting personal data, BCP has a responsibility to ensure that it is handled in an efficient and ethical manner. The purpose of this document is to guide the practice of BCP staff in relation to client confidentiality and data protection.

1.1 Policy Statement

All organisations have an obligation to keep information 'safe and secure' and have appropriate measures in place to prevent "unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction" in compliance with sections 2(1)(d) and 2C of the Data Protection Acts 1988 & 2003.Ballyfermot Chapelizod Partnership respects the right to confidentiality of all clients of our service and commits to handling all client data securely in line with relevant legislation. Information about BCP clients is shared with similar not-for-profit organisations and relevant government departments to facilitate better service delivery. This is done on a need-to-know basis and with the informed consent of clients as agreed during the registration process.

1.2 Relevant Legislation

The Following pieces of legislation[1] are relevant in the area of confidentiality and data protection;

- Data Protection Act 1988 & 2003
- Freedom of Information Acts 1997 and 2003
- Garda Vetting Bureau Act 2012
- Criminal Law Act 1997
- Criminal Justice (Withholding of Information on offences against Children and Vulnerable Persons) Act 2012

1.3 Key Principles

Under the Data Protection Acts 1988 & 2003, Ballyfermot Chapelizod Partnership as data controllers have a legal responsibility to;

- Obtain and process personal data fairly
- Keep it only for specified and lawful purposes
- Process it only in ways compatible with the purposes for which it was initially given
- Keep personal data safe and secure
- Keep data accurate, complete and up-to-date
- Ensure that it is adequate, relevant and not excessive
- Retain it no longer than is necessary for specified purposes
- Provide a copy of his/her personal data to any individual, on request.

Section 2: Confidentiality & Data Protection Procedures

2.1 General Procedures

This section sets out procedures in a number of specific areas where particular attention must be paid in order to protect the confidentiality of personal data held by Ballyfermot Chapelizod Partnership. There are, however, a number of general procedures which staff should follow;

[1] All relevant legislation is accessible at www.irishstatutebook.ie

- Access to rooms where personal information is stored is restricted only to those staff members that have permission to work there. All such rooms are secured by locks when staff members are not present.

- Access to systems which are no longer in active use and which contain personal data will be removed where such access is no longer necessary or cannot be justified

- Passwords used to access PCs, applications, databases, etc. must be of sufficient strength to deter password cracking or guessing attacks. A password must include numbers, symbols, upper and lowercase letters. Passwords should have a minimum of 8 characters. Passwords based on repetition, letter or number sequences, usernames, or biographical information like names or dates must be avoided.

- Staff who retire or resign from Ballyfermot Chapelizod Partnership are removed immediately from mailing lists and access control lists. Relevant changes must also occur if a staff member is transferred to another role internally. It is the responsibility of the individual's line manager to ensure this is carried out.

- Contractors, consultants and external service providers employed by BCP are subject to strict procedures with regard to accessing personal data by way of formal contract in line with the provisions of the Data Protection Acts.

- New staff are familiarised with BCP confidentiality and data protection procedures as part of the induction process before being allowed to access confidential or personal data.

- All staff must ensure that PCs are logged off or 'locked' when left unattended for any period of time (e.g. in Windows, using Ctrl+Alt+Del keys). Staff are restricted from saving files to the local disk and are instructed to only save files to their allocated network drive.

- All BCP staff should exercise caution in their use of the Personal Public Service Number (PPSN) in systems, on forms and documentation. There is a strict statutory basis providing for the use of the PPSN. This allows organisations use the PPSN in support of a provision of a public service to a customer. The Department of Social Protection manages the issuance and use of PPS Numbers. A register of organisations that use the PPSN has been prepared and published to promote transparency regarding the ongoing use and future development of the PPSN as a unique identifier for public services. The register is available via: http://www.welfare.ie/en/Pages/Personal-Public-Service-Number-Register-of-Users.aspx. BCP staff must only share PPSN numbers of clients for an agreed purpose and PPSN's should only shared with agencies on this register. All documents containing client PPSN's must be shredded when no longer in use.

2.2 Protocols for the collection of personal data on young people under 18

The minimum age at which a person can give consent to having their personal data processed is not specified in the Data Protection Acts. Section 2A (1) of the Acts provides that, where a person by reason of his or her physical or mental incapacity or age, is or is likely to be unable to appreciate the nature and effect of giving consent, such consent may be given by a parent or guardian or a grandparent, uncle, aunt, brother or sister of the person provided that the giving of such consent is not prohibited by law. Where a person is under the age of 18, the Acts require the data controller to make a judgement on whether the young person can appreciate the implications of giving consent.

As a general rule, BCP accepts consent from individuals over 16 years of age. Where the individual is under 18, the consent of a parent or guardian is obtained and suitable authentication measures adopted to make sure that such consent is genuine. In relation to the right of access to data, staff must use professional judgement on a case by case basis, on whether the entitlement to access

should be exercisable by (i) the individual alone, (ii) a parent or guardian alone, or (iii) both jointly. In making a decision, particular regard is given to the maturity of the young person concerned and his or her best interests.

2.3 Paper Records

The following guidelines have been adopted by Ballyfermot Chapelizod Partnership regarding the use and storage of paper files containing personal data;

- The first step to setting up a file is the population of the registration form, ensuring that the client signs the form confirming they have received and understand the Confidentiality Statement and give their consent to the use and disclosure of client information as outlined in the Confidentiality Statement (See Appendix 1).

- Once the client has been established on CSS/IRIS /CRM or other databases as required by funders thus allowing their information to be retrieved electronically, files are stored in the central filing system in each office

- If a BCP officer needs to retain a file for any reason (e.g. processing training) files should be stored alphabetically in BCP officers' desk and moved to the central filing system as soon as the purpose for which it is retained has been achieved

- Where documents containing personal data are no longer needed (e.g. registration forms copied for data entry purposes) they will be securely disposed of using the shredding machines available in each office.

- Personal and sensitive information held on paper must be inaccessible to callers to offices; this is done through restricting access to rooms where clients' files are stored including pin-pad locks and locks on individual rooms.

- For those clients involved in the guidance process, the central filing area is the admin room in Drumfinn (Orchard meeting room) the TUS office in Cheery orchard and EGO office in Decies road.

- Files for those clients active in the Enterprise process are filed alphabetically in the Enterprise office

- Files for clients who have progressed onto the Back to Work Enterprise Allowance are filed alphabetically in the year they start for three years before being moved to storage

- Where a client is working across a number of sections, whoever is actively working with the client is responsible for the management of the file

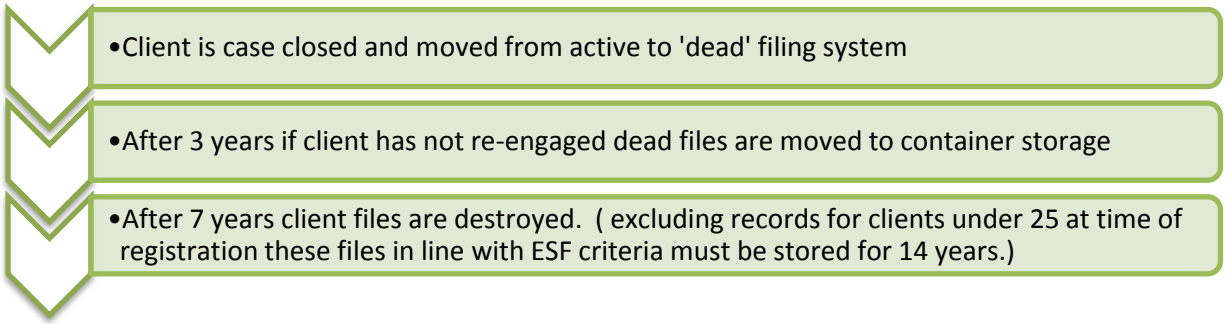
- When paper files are transferred between staff or BCP departments this usually entails hand delivery. Attention must be paid to ensuring security of personal data where staff transport files between offices. Staff should never remove client files from the offices of BCP unless for there is a clear business purpose and prior approval from the relevant line manager.

- There should be no duplication of client files

2.2.1 Retention and Disposal of Paper Files

In line with the Key Principles outlined in section 1.2 of this document, BCP retains client records no longer than is necessary for specified purposes. BCP's current procedures are to retain inactive paper records for a period of 7 years before shredding. Where litigation may potentially arise in the future (e.g. in relation to accidents/personal injuries involving employees/clients or accidents occurring on BCP property), the relevant records should be retained until the possibility of litigation ceases.

The statute of limitations in relation to personal injuries is currently two years. The limitation period for other causes of action varies, but in most cases is not greater than six years. A limitation period does not begin to run until the person concerned acquires knowledge of the facts giving rise to the claim. In the case of minors, the limitation period does not begin to run until they reach their 18 birthday or later if the date of knowledge post dates their 18th birthday. It would appear prudent not to destroy records likely to be relevant in litigation at least until the six year limitation period has expired. Current procedures for the disposal of paper files are contained in Figure 1 below however files may be retained for longer periods if this is a contractual requirement of BCP funders.



2.4 Electronic Records & Email

Along with paper files personal data is stored electronically in a number of systems across the organisation. Electronic records include (but are not limited to); Department of Social Protection (BOMI), Pobal's IRIS system, TUS one view, BCP SharePoint, BCP CRM, MS Office Spreadsheets, Word Documents, Excel and Access Databases. The Ballyfermot Chapelizod Partnership's network consists of a single Microsoft Server running server 2012 R2 Domain distributed across 3 buildings (Drummfinn, Decies office and Cherry orchard). Email is via Microsoft office 365 and is held in the cloud under encryption. Both offices are protected by Zyxel SonicWALL Unified Threat Management UTM Firewalls. To protect against ransom ware we also have Sophos Intercept X software. Key considerations on the security of electronic records include

- Where personal or sensitive data is held on applications and databases, relevant IT security and access controls must be in place. All electronic records of client personal information are protected by passwords meeting the criteria in section 2.1 (3) and these passwords are only be available to staff with a business need to access these records.

- Access to files containing personal data is monitored by supervisors on an ongoing basis. All staff members are made aware that this is being done.

- Standard unencrypted email should never be used to transmit any data of a personal or sensitive nature. Staff that wish to use email to transfer such data must ensure that personal or sensitive information is encrypted either through file encryption or through the use of a *secure email* facility which will encrypt the data (including any attachments) being sent. Staff should also ensure that such email is sent only to the intended recipient[2].

[2] The encryption methods available are currently under review with enhanced email security due to be implemented in before the end of 2017.

- All computer equipment (especially storage media) will be disposed of securely at end of life or returned to funders if contractually stipulated.

- All BCP offices are protected by Zyxel SonicWall Next Generation UTM firewalls. These are kept in Licence with Zyxel SonicWall Comprehensive Gateway Security. This includes:
  - Sophos Anti Spyware Protection
  - Sophos Anti Virus Protection
  - Sophos Intrusion Prevention and Detection
  - Sophos Content Filter
  - Sophos Intercept X software
  -
- All SonicWall firewalls are managed and monitored in real time by BCP IT contractors. This is done using Zxyel Global Management System (GMS). GMS allows the real-time monitoring of systems to identify potential threat activity, bandwidth usage and web usage.

2.5 Remote Access

Business needs may require that some staff be able to access email and BCP servers while working off-site. All requests for remote access must be considered by the Management Team and a decision will be made to grant access where there is a clear business need and appropriate risk management systems in place. The following guidance should be adhered to by staff granted remote access to BCP servers;

- Data that is available via remote access should not be copied to staff members personal PCs or to portable storage devices, such as laptops, memory sticks, etc. that may be stolen or lost

- When accessing this data remotely, it must be done via a secure encrypted link (e.g. IPSEC or SSL VPN tunnel) with relevant access controls in place;

- Additional stringent security and access controls should be in place, e.g. the mandatory use of strong passwords and security token authentication (i.e. twofactor authentication)

- Staff should be aware that it is imperative that any wireless technologies/networks used when accessing BCP systems should be encrypted to the strongest standard available.

Remote Access can be revoked at any time at the discretion of BCP Management Team.

2.6 Laptops and Other Mobile Storage Devices (incl. Mobile Phones, PDAs, USB memory sticks, External Hard Drives, etc.)

The use of laptops, USB memory sticks and other portable or removable storage has increased substantially in the last number of years. Likewise, the use of personal communications and storage devices such as mobile phones, PDAs, etc. has also increased. These devices are useful tools to meet the business needs of staff. They are, however, highly susceptible to loss or theft. To protect the content held on these devices, the following recommendations should be followed:

- Personal, private, sensitive or confidential data should not be stored on portable devices unless absolutely necessary. Staff are not permitted to store client data on mobile devices unless there is a clear business reason and express permission is given in writing by their line manager. In cases where this is unavoidable, all devices containing this type of data must be encrypted. With regard to laptops, full disk encryption must be employed regardless of the type of data stored.

- All portable devices should be password-protected to prevent unauthorised use of the device and unauthorised access to information held on the device. In the case of mobile phones, both a PIN and login password should be used. Manufacturer or operator-provided PIN codes must be changed from the default setting by the user on receipt of the device;

- Passwords used on these devices should be of sufficient strength to deter password cracking or guessing attacks. Passwords used for mobile devices are subject to the guidelines in section 2.1 (3) above.

- Data held on portable devices are backed up regularly to BCP internal servers

- When portable computing devices are being used in public places, care must be taken to avoid unwitting disclosure of information, e.g. through overlooking or overhearing by unauthorised persons

- Portable devices must not contain unauthorised, unlicensed or personally licensed software. All software must be authorised and procured through BCP's IT contractors Definitive Solutions

- Anti-virus/Anti-spyware/Personal Firewall software must be installed and kept up to date on portable devices. These devices should be subjected to regular virus checks using this software

- Laptops and other mobile devices must be physically secured if left in the office overnight. When out of the office, the device should be kept secure at all times

- Portable devices containing BCP data should never be left in an unattended vehicle

Section 3: Procedures for Sharing Client Data

The sharing of information with external agencies is necessary for many aspects of the work of Ballyfermot Chapelizod Partnership. This section provides guidance for the sharing of BCP client data with external agencies.

3.1 Who has acess to BCP client data

Aside from the specific staff member(s) providing BCP services to the client the following agencies have access to BCP client data;

- The Department of Social Protection (DSP) use BCP client information to monitor the engagement of clients with the job seeking process
- BCP funders may access client files for audit purposes
- BCP staff may share client information for the purpose or referral to other service providers (e.g. educational institutions, training providers, potential employers, funding sources etc.) All BCP clients are informed of the procedures for sharing information about them with other agencies as part of the registration process.
- In line with the Freedom of Information Acts 1997 and 2003 BCP clients have the right to view the data held about them at any reasonable time. This can be done by written request to the manager of the relevant department. In addition clients have the right to have any incorrect information amended on request.

3.2 What information is shared & for what purpose

Client information that may be shared with external agencies named above includes

- PPS. No.

- Contact details i.e. name, address, phone number & date of birth
- Target group membership, gender and nationality
- Date of appointments, phone calls and letters
- Attendance/non attendance for appointments and notes of conversations and agreements
- Personal Action Plan and updated implementation of same
- Employment history and educational standards
- Curriculum Vitae
- Referrals to training / education/ employment health services
- Job Placement including self employment

Information is shared for the following purposes;

- Processing Applications and supporting client progression
- Compiling statistical information to plan and improve BCP services
- Analysing information about BCP service users for funders and producing BCP statistics for publication

3.4 Limits of Confidentiality

On registering with Ballyfermot Chapelizod Partnership, clients are advised that their information will be stored safely and securely with a strong focus on confidentiality and data protection. Nonetheless there are limits to client confidentiality and personal information can and will be shared with the relevant statutory authorities in the following four circumstances[3];

A A client demonstrates suicidal ideation or there is evidence of intent to seriously harm self or others.

1. **A client demonstrates suicidal ideation or there is evidence of intent to seriously harm self or others.**
   If a BCP staff member believes there is a substantive threat of harm to self or others, the staff member is obliged to contact a family member / ambulance / Gardai as appropriate.

2. **A client reveals information that suggests a child may be at risk of one of the four categories of child abuse**
   In line with National Guidance for the Protection and Welfare of Children, BCP staff have an obligation to pass on concerns about the safety and welfare of children to the organisation's Mandated Person, who will take appropriate action in referring onto Tusla social work staff and/or the Gardai. For more information consult BCP Policies and Procedures for the Protection of Children and Vulnerable Adults.

3. **A BCP staff member is ordered by a court of law to give evidence in relation to a client**
   A court of law by way of a judicial subpoena can demand that a staff member appear in court to give evidence in relation to their contact with a client. It is important that a line manager, who will offer and/or seek support as appropriate, supervises all dealings with the judicial system

4. **A client discloses involvement in a crime or plans to commit a crime**
   Withholding information is an offence under the Criminal Law Act 1997, section 7(2). If possible, the staff member should inform the client of this prior to any disclosure being made. If a disclosure is made on this issue, it should immediately be discussed with the staff member's line manager.

[3] For further information on each of the above points please refer to TAP Policy and Procedures for the Protection of children and vulnerable adults (2014)

Key Message: Information shared with the appropriate statutory authorities for the purpose of the protection of children or vulnerable adults is not a breach of data protection or confidentiality.

Section 4: Breaches of Confidentiality and Data Protection

4.1 Breach Management Procedures

A data security breach can happen for a number of reasons, including:

- Loss or theft of data or equipment on which data is stored (including break-in to an organisation's premises)
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as a flood or fire
- A hacking attack
- Access where information is obtained by deceiving the organisation that holds it.

There are five elements to any breach management plan

- Identification and Classification
- Containment and Recovery
- Risk Assessment
- Notification of Breach
- Evaluation and Response

4.1.1 Identification and Classification

On becoming aware of an information security incident staff members have an obligation to bring it to the attention of their line manager as soon as possible. Having such a procedure in place allows for early recognition of the incident so that it can be dealt with in the most appropriate manner.

Details of the incident should be recorded accurately, including the date and time the incident occurred, the date and time it was detected, who/what reported the incident, description of the incident, details of any ICT systems involved, corroborating material such as error messages, log files, etc. In this respect, staff members need to be made fully aware as to what constitutes a breach.

4.1.2 Containment and Recovery

Containment involves limiting the scope and impact of the breach of data protection procedures. If a breach occurs the relevant line manager in consultation with the Senior Management team should;

- decide on who would take the lead in investigating the breach and ensure that the appropriate resources are made available for the investigation
- establish who in the organisation needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. For example, this might entail isolating a compromised section of the network, finding a lost file or piece of equipment, or simply changing access codes.
- establish whether there is anything that can be done to recover losses and limit the damage the breach can cause
- where appropriate, inform the Gardai.

4.1.3 Risk Assessment

In assessing the risk arising from a data security breach, the Management Team should consider what would be the potential adverse consequences for individuals, i.e. how likely it is that adverse consequences will materialise and, in the event of materialising, how serious or substantial are they likely to be. In assessing the risk, Departments should consider the following points:

- what type of data is involved?
- how sensitive is it?
- are there any protections in place (e.g. encryption)?
- what could the data tell a third party about the individual?
- how many individuals' personal data are affected by the breach?

4.2 Notification of Breaches

Although there is no current explicit legal obligation to notify individuals or other bodies under the Data Protection Acts of a breach, the Data Protection Commissioner's Office encourages voluntary notification and early engagement with the Office. Therefore, if inappropriate release/loss of personal data occurs it should be reported immediately, both internally and to the Data Protection Commissioner's Office and, if appropriate in the circumstances, to the persons whose data it is and the relevant funders e.g. Department of Social Protection if contractually obliged to do so.

When notifying individuals, the Management Team should consider using the most appropriate medium to do so. They should also bear in mind the security of the medium used for notifying individuals of a breach of data protection procedures and the urgency of the situation. Specific and clear advice should be given to individuals on the steps they can take to protect themselves and what Ballyfermot Chapelizod Partnership is willing to do to assist them.

Departments should also provide a way in which individuals can make contact for further information, e.g. a phone number, information on BCP website etc.

The Office of the Data Protection Commissioner will provide advice upon notification as to the requirement or otherwise, in particular circumstances, to notify individuals.

4.2.1 Evaluation and Response

Subsequent to any information security breach a thorough review of the incident should occur. The purpose of this review is to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.

Any recommended changed to policies and/or procedures should be documented and implemented as soon as possible thereafter.

Appendix 1: Confidentiality Statement

In registering with the Ballyfermot Chapelizod Partnership (BCP) you consent to become a client of BCP. As a client of BCP we will hold information provided by you in *two* ways:

1. **On a client registration form**
2. **In an electronic database**

The client registration form is signed by you as a client. This gives permission to BCP personnel to work on your behalf to help you progress towards training, education and employment opportunities (Including Self Employment) and volunteering opportunities.

. **The information we record is used for the following purposes:**

- Processing Applications
- Compiling statistical information to help us plan and improve our service
- Analysing information about service users for our funders and producing our own statistics for publication

The following information is stored:

- PPS. No.
- Contact details i.e. name, address, phone number & date of birth
- Target group membership, gender and nationality
- Date of appointments, phone calls and letters
- Attendance/non attendance for appointments and notes of our conversations and agreements
- Personal Action Plan and updated implementation of same
- Employment history and educational standards
- Referrals to training / education/ employment
- Job Placement including self employment

Who will see it and what is it used for

- To ensure continuity of service should you engage with any other employment service
- The Department of Social Protection (DSP) may use this information to monitor your engagement with the job seeking process
- Our funders may review your file for audit purposes.
- You may view your paper file at any reasonable time, upon written request to designated BCP Personnel.
- Files are shredded when a client has had no contact with the service for six years.

.

Note

- The Ballyfermot Chapelizod Partnership follow procedures necessary to protect children and vulnerable adults – If we are concerned that a child or vulnerable adult is being harmed or at risk of being harmed we are obliged to report this to the HSE, Tusla or the Gardai.
- If through your engagement with our staff, they believe there to be a clear risk of you causing physical harm to yourself or others we will be obliged to contact a responsible adult of your choosing or the Gardai.