Phoenix Community Care Ltd
Policy & Procedure

0223 – Data Protection

(Including Confidentiality, Access to Records, Retention of Records & GDPR)

Version	Written	Updated/ Reviewed	Scheduled Review Date	Author/ reviewer	Approving Body	Date Approved
1	Oct 2013		Oct 2014	J A Coates	PCC Foster Directos	5.2.14
		Jan '15	Jan '16	J A Coates	PCC directors	Feb '15
		July '16	Juy'19	J A Coates	PCC Directors	July '16
2	Nov 2018			G Areola	PCC Directors	Nov '18

Contents

INTRODUCTION

Phoenix Community Care (PCC) has to collect and use information about people with whom we work. This personal information is handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means.

We regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we carry out business. We will ensure that we treat personal information lawfully and correctly.

To this end we fully endorse and adhere to the principles of the General Data Protection Regulation (GDPR).

This policy applies to the processing of personal data in manual and electronic records kept by us in connection with our human resources function as described below. It also covers our response to any data breach and other rights under the GDPR.

This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

DEFINITIONS

“Personal data” is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person’s name, identification number, location, online identifier. It can also include pseudonymised data.

“Special categories of personal data” is data which relates to an individual’s health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

“Criminal offence data” is data which relates to an individual’s criminal convictions and offences.

“Data processing” is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

DATA PROTECTION PRINCIPLES

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

a) processing will be fair, lawful and transparent
b) data be collected for specific, explicit, and legitimate purposes
c) data collected will be adequate, relevant and limited to what is necessary for the purposes of processing
d) data will be kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
e) data is not kept for longer than is necessary for its given purpose
f) data will be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
g) we will comply with the relevant GDPR procedures for international transferring of personal data

TYPES OF DATA HELD

We keep several categories of personal data on our employees in order to carry out effective and efficient processes. We keep this data in a personnel file relating to each employee and we also hold the data within our computer systems, for example, our holiday booking system.

Specifically, we hold the following types of data:

a) personal details such as name, address, phone numbers
b) information gathered via the recruitment process such as that entered into a CV or included in a CV cover letter, references from former employers, details on your education and employment history etc
c) details relating to pay administration such as National Insurance numbers, bank account details and tax codes
d) medical or health information
e) information relating to your employment with us, including:

i) job title and job descriptions
ii) your salary
iii) your wider terms and conditions of employment
iv) details of formal and informal proceedings involving you such as letters of concern, disciplinary and grievance proceedings, your annual leave records, appraisal and performance information
v) internal and external training modules undertaken

All of the above information is required for our processing activities. More information on those processing activities are included in our privacy notice for employees, which is available from your manager.

EMPLOYEE RIGHTS

You have the following rights in relation to the personal data we hold on you:

h) the right to be informed about the data we hold on you and what we do with it;

i) the right of access to the data we hold on you. More information on this can be found in the section headed “Access to Data” below and in our separate policy on Subject Access Requests”;
j) the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as ‘rectification’;
k) the right to have data deleted in certain circumstances. This is also known as ‘erasure’;
l) the right to restrict the processing of the data;
m) the right to transfer the data we hold on you to another party. This is also known as ‘portability’;
n) the right to object to the inclusion of any information;
o) the right to regulate any automated decision-making and profiling of personal data.

More information can be found on each of these rights in our separate policy on employee rights under GDPR.

RESPONSIBILITIES

In order to protect the personal data of relevant individuals, those within our business who must process data as part of their role have been made aware of our policies on data protection.

We have also appointed employees with responsibility for reviewing and auditing our data protection systems.

LAWFUL BASES OF PROCESSING

We acknowledge that processing may be only be carried out where a lawful basis for that processing exists and we have assigned a lawful basis against each processing activity.

Where no other lawful basis applies, we may seek to rely on the employee’s consent in order to process data.

However, we recognise the high standard attached to its use. We understand that consent must be freely given, specific, informed and unambiguous. Where consent is to be sought, we will do so on a specific and individual basis where appropriate. Employees will be given clear instructions on the desired processing activity, informed of the consequences of their consent and of their clear right to withdraw consent at any time.

ACCESS TO DATA

As stated above, employees have a right to access the personal data that we hold on them. To exercise this right, employees should make a Subject Access Request. We will comply with the request without delay, and within one month unless, in accordance with legislation, we decide that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit.

No charge will be made for complying with a request unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request. In these circumstances, a reasonable charge will be applied.

Further information on making a subject access request is contained in our Subject Access Request policy.

DATA DISCLOSURES

The Company may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

p) any employee benefits operated by third parties;
q) disabled individuals - whether any reasonable adjustments are required to assist them at work;
r) individuals' health data - to comply with health and safety or occupational health obligations towards the employee;
s) for Statutory Sick Pay purposes;
t) HR management and administration - to consider how an individual's health affects his or her ability to do their job;
u) the smooth operation of any employee insurance policies or pension plans;
v) to assist law enforcement or a relevant authority to prevent or detect crime or prosecute offenders or to assess or collect any tax or duty.

These kinds of disclosures will only be made when strictly necessary for the purpose.

DATA SECURITY

All our employees are aware that hard copy personal information should be kept in a locked filing cabinet, drawer, or safe.

Employees are aware of their roles and responsibilities when their role involves the processing of data. All employees are instructed to store files or written information of a confidential nature in a secure manner so that are only accessed by people who have a need and a right to access them and to ensure that screen locks are implemented on all PCs, laptops etc when unattended. No files or written information of a confidential nature are to be left where they can be read by unauthorised people.

Where data is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Employees must always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.

Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless prior authorisation has been received. Where personal data is recorded on any such device it should be protected by:

a) ensuring that data is recorded on such devices only where absolutely necessary.
b) using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted.
c) ensuring that laptops or USB drives are not left where they can be stolen.

Failure to follow the Company's rules on data security may be dealt with via the Company's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

THIRD PARTY PROCESSING

Where we engage third parties to process data on our behalf, we will ensure, via a data processing agreement with the third party, that the third party takes such measures in order to maintain the Company's commitment to protecting data.

INTERNATIONAL DATA TRANSFERS

The Company does not transfer personal data to any recipients outside of the EEA.

REQUIREMENT TO NOTIFY BREACHES

All data breaches will be recorded on our Data Breach Register. Where legally required, we will report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach.

More information on breach notification is available in our Breach Notification policy.

TRAINING

New employees must read and understand the policies on data protection as part of their induction.

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data controller/auditors/protection officers for the Company are trained appropriately in their roles under the GDPR.

All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals

and the Company of any potential lapses and breaches of the Company's policies and procedures.

RECORDS

The Company keeps records of its processing activities including the purpose for the processing and retention periods in its HR Data Record. These records will be kept up to date so that they reflect current processing activities.

DATA PROTECTION COMPLIANCE

Our Data Protection Officer is:

Mr Gareth Hawkes
gareth@phoenixcommunity.org

Records – Preservation, Retention and Destruction

Scope

This policy applies to all PCC Foster Care Agency's employees, including:
• Permanent staff
• Voluntary staff
• Placements and Work Experience
• Temporary staff

Purpose

To inform staff of the PCC Foster Care Agency and PCC Supported Housing requirements in relation to retention and destruction and what is expected of them.
To ensure that PCC Foster Care Agency and PCC Supported Housing comply with the relevant legislation and codes of practice.

Introduction

PCC Foster Care Agency and PCC Supported Housing are committed to fulfilling its duties and responsibilities in regard to the preservation, retention and destruction of the records as outlined in the:

- Foster Service Regulation 2011 (Sections 22, 30, 31, 32)
- Foster Services: National Minimum Standards 2011 (Standard 26)
- Data Protection Act 1998
- Freedom of Information Act 2000 (Section 46)
- Public Records Act 1958.
- Common Law on Confidentiality

This document will apply to all information recorded and held by PCC Foster Care Agency, both corporate, health records and service user's records in any format. This document provides the procedures for the preservation, retention and destruction of all records.
Common Law on Confidentiality

Responsibilities

Directors

PCC Directors have overall responsibility for record management in PCC. As the accountable persons they are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

PCC has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

Departmental Managers

Departmental Managers are responsible for raising issues to the PCC board of Directors as appropriate.

All members of staff

Must be aware of this policy and store and destroy records according to this policy and procedure.

Storage of personal data

Locked cabinets

All personal data whether that of Directors, employees, foster carers, looked after children, service users or any of persons linked to PCC, will be stored in filing cabinets or cupboards that are lockable and only authorised personnel will hold the keys.

Electronic storage

All personal data whether that of Directors, employees, foster carers, looked after children, service users or any of persons linked to PCC, will be stored on the company's Google Drive which is password protected. Access is only given as needed.

Third party storage management

PCC Foster Care Agency uses Charms (Social Care Network Solutions Ltd), password and passcode protected.

PCC Human Resources uses HR Online (©Peninsula Business Services Limited), Password protected.

Preservation, retention and destruction of records

Retention and destruction schedule

PCC Foster Care Agency and PCC Supported Housing has an approved retention and destruction schedule in place that identifies the retention periods for a number of records.

The retention and destruction schedule should be regularly reviewed but as a minimum at least every two years. Details of the schedule are included in this document.

Appraisal of records

Records should be appraised in line with the Retention and Destruction Schedule to determine whether they should be retained or destroyed.

Records for permanent preservation

If material is in a category selected for permanent preservation, the original document must be preserved.

The records that should be permanently preserved are indicated in the Retention and Destruction Schedule.

Records that are the subject of a request for information under the Freedom of Information Act 2000

It is essential that all records that are the subject of a request for information under the Freedom of Information Act 2000 should be retained until the processing of the request for information is completed.

Destruction of records that are not identified on the Retention and Destruction Schedule

For all records that need to be destroyed, that are not identified on the Retention and Destruction Schedule, a review should take place as to whether the record should be retained.

The Directors should be contacted and if the destruction of the record(s) is appropriate they will authorise the destruction. The Departmental Manager will log all decisions to destroy the records, recording:

- the title and description of the record
- the date of the request to destroy the record
- the reason destruction has been requested
- the date authorisation was given to destroy the record.

Destruction of electronic records

Records held in a network folder/ email server must be deleted from the system (and from the recycle bin). For records held on mobile devices, if the mobile device is being reused then the record should be simply deleted from the device. If the device and its records are no longer of any use, it must be disposed of securely.

Destruction of paper records

Paper records that contain personal identifiable or business confidential information must be destroyed securely by:

- shredding

Records that are not confidential can be destroyed locally in waste bins.

PCC retention and destruction schedule

General

- Minute books/files will be kept forever. These are legal documents and must not be destroyed. These will be kept in a secure cabinet/storage area or scanned and kept in the google drive.
- Title deeds, leases, agreements etc. will be kept whilst the organisation owns/occupies property/land. These will be kept in a secure cabinet/storage area.
- Insurance documents, Certificates of Employer's Liability and Public Liability will be kept as required by law, which is currently 40 years.
- The organisation will keep documents as required by individual funders.

Statutory accounts and all supporting paperwork

- Statutory accounts and all supporting documentation are to be retained for six years plus the current year.

HR records retention period

- Application forms for candidates are to be retained for six months after notifying the unsuccessful candidate.
- Application forms – duration of employment.
- References obtained from third parties – one year.
- Sickness and leave records – three years after the end of each tax year.
- Statutory maternity pay records to be retained for three years after the end of the tax year in which the maternity period ends.
- Records relating to accident or injury at work – three years.
- Annual appraisal records – five years.
- Redundancy details to be retained six years after employment has ceased.
- Promotion, transfer, training and disciplinary records – one year from end of employment.
- Payroll records, P45, other HMRC documentation and forms to be retained for six years plus current year.
- Personnel file will be retained for two years after employment terminates. After this time the file will be destroyed and a summary or record of service e.g. name, position held, dates of employment, etc. will be retained for ten years from end of employment. This will include references given or details retained to enable reference to be provided for future employment.

Records of Looked After Children

Files of children who are looked after, or who cease to be looked after before the age of 18 years, should be retained completely intact until the 18th birthday is reached.

When children who have previously been looked after reach the age of 18 or they cease being looked after at 18 take the following actions immediately:

• Examine the file and give any personal document to the child. This will include birth and baptismal certificates, photographs and any other documents that help to support a sense of identity. In the case of a deceased child, these documents should be given to the parents or next of kin where this is considered appropriate.
• Remove and destroy all documents on the file, which are of a routine nature including forms relating to such matters as clothing, employment, and holidays. Provide evidence of such destruction in list form to be recorded as "Routine culling of (describe which type of documents) took place on... (insert date) by… (insert name)". In addition, destroy documents that duplicate information already recorded elsewhere on the file.
• Retain the file for 75 years from the child's date of birth OR, if the child has died before attaining the age of 18, for the period of 15 years from the date of death or at the age of 18 whichever is the later. As soon as the case is closed, store the files by:

- Scanning them into a named file on the computer
- Condense the file
- Save the file in 'Archived Files'
- Record the person's name, DOB, when they came into the care of PCC and When they moved on from PCC, on the spread sheet entitled past clients.
- The paper file will then be archived in the attic.

Records of Foster Carers

The retention period for records of foster carers is 10 years after approval has ended under satisfactory circumstances. As soon as approval has ended, all existing material and records should be archived by:

- Scanning them into a named file on the computer
- Condense the file
- Save the file in 'Archived Files'
- Record the person's name, DOB, when they came into the care of PCC and When they moved on from PCC, on the spread sheet entitled 'Past Clients'.
- The paper file will then be archived in the attic.

Destruction of records

Once a record has surpassed the required retention period it should be destroyed and logged in the following manner:

- All paper records should be shredded.
- All electronically saved files should be deleted
- The person's entry on PCC's spreadsheet entitled 'Past Clients' should now contain the entry 'File Destroyed'.

All electronic records and files are regularly backed up and if and when PCC's systems are updated all files and records are transferred and this policy and procedure will be updated to include any changes in procedure. When a file is destroyed it is removed from the master file and any copied or backed up systems that may exist.

Access to Records

Scope

This policy applies to all PCC Foster Care Agency and PCC Supported Housing employees, including:

• Permanent staff
• Voluntary staff
• Placements and Work Experience
• Temporary staff

Purpose

To ensure that service users and carers are enabled to access their records in compliance with the Data Protection legislation and that staff are consistent in their approach to access of files.

Introduction

PCC Foster Care Agency and PCC Supported Housing are committed to fulfilling its duties and responsibilities as described in the statutory framework including:

- The Data Protection Act 1998
- General Data Protection Regulations 2018
- The Crime and Disorder Act 1998, Section 115
- The Human Rights Act 1998
- The Freedom of Information Act 2000

The Data Protection Act applies to all personal information within the relevant definitions of the Act and as further defined by court decisions.

Rights of Access

Under the terms of the Data Protection Act any living person has a right to access to personal information about themselves. Where access is denied the individual may refer this to the data protection officer or PCC Directors.

Service Users have free informal access to information held on them.

When dealing with other agencies or individuals it is important to ask them if the jointly held information can be shared with the service user.

Formal access to closed and open files will be provided free of any charge.

Requests for personal information will need to be authenticated before allowing access. An individual should provide at least two proofs of identity such as a passport, driving license and utilities bill with an address. If this person is a current

service user then a key worker can complete authentication and if necessary accompanied by a signed letter on PCC Letterhead.

Individuals can apply for access to their personal information through a key worker or, if they have left the service of PCC, a representative who will need to be verified. See below for further details.

Requests made by, or on behalf of, a child

Where a child or young person under the age of 18 years makes a request for access to their information, the Key Worker / Internal Social Worker, together with relevant case workers, must decide whether or not he/she has sufficient understanding to do so. That is, does he/she understand the nature of the request? If so, then the request for access should be complied with.

If a child does not have sufficient understanding to make his/her own request, a carer / social worker can make the request on the child's behalf or the service user's social worker. In this case the status of the person making the request will need to be verified.

Where the Key Worker / Internal Social Worker and the case worker considers that granting access to a carer / social worker is likely to result in serious harm to anyone or is not in the child's best interest, they may refuse access. The reasons for refusal must be recorded in writing and included in the child's file. In this case the carer / social worker may then apply to the County Council's Data Protection Officer or the Information Commissioner, or the court for access. That decision should also be circulated the data protection officer and all PCC Directors

Requests on behalf of a person lacking mental capacity

If a person over 18 years of age with a mental illness has legal capacity i.e. she/he understands the nature of the request, she/he can request access.

If a person lacks capacity to manage their affairs, someone acting under an order of the Court of Protection or acting within the terms of a registered Enduring Power of Attorney can request access on his/her behalf. Mental order does not necessarily equate with mental incapacity.

Disclosure to social care staff

Access to personal information will be made available to the designated employees with responsibility to prepare the files for access or for whom the information is necessary in order to carry out the service within Social Care settings and to meet statutory and legal obligations.

Disclosure to councillors

Personal information about service users is not automatically available to Councillors on Scrutiny Committees. However, a Councillor does have a common law right to inspect information in the possession of the authority if it is reasonably necessary for the performance of his/her duties.

The Director of the Service Grouping will be informed of all such requests and will also be required to authorise any disclosures to Councillors who are not members of Scrutiny Committees.

Disclosure to research workers

In considering requests from research workers for personal information, the following principles will apply:

All research activity should be subject to ethical review. The degree of ethical scrutiny will be proportionate to the likely risks to services users and others involved in the research process

The information will only be used in a manner which is consistent, with benefit to people and will not be used in a manner which may cause damage or distress to the person

The personal information used in statistical research will not be processed to support measures or decisions with respect to particular individuals

Wherever possible, the consent of the person will be obtained

Adoption information will not be disclosed to researchers unless the above principles are applied and authorisation has been gained in writing by the Secretary of State to obtain such information under regulations 15.2.6 of the Adoption Act Regulations 1983

Disclosure to other agencies and organisations

Information may only be disclosed to other agencies if there is a valid, signed and up to date Information Sharing Protocol.

Section 115 of The Crime and Disorder Act 1998 enables all relevant authorities (the Partners) to disclose information between them for the purpose of the Act, which is to tackle crime and disorder to create safer communities. The presumption of confidentiality will, however, still apply. PCC will therefore need to make objective assessments of all the available information to determine whether disclosure is justified by public interest or in the interest of safeguarding a child.

In considering requests for access the best interests of the service user or carer must be borne in mind, especially where access is being given without the direct consent of the service user or carer. If there is any doubt about whether or not to give access to all or part of any record the Data Protection Officer and Legal Services should be consulted.

Withholding information

Certain personal information is exempt from the disclosure requirements of the Data Protection Act. The exceptions are:

Prevention of Crime etc.

The authority need not disclose information to the service user or person requesting the file on behalf of the service user which is held for the purposes of the prevention or detection of crime, or to apprehend or prosecute offenders if disclosure would be likely to prejudice one of these purposes.

Risk of Serious harm.

The authority need not disclose information to the service user or person requesting the file on behalf of the service user if it believes this would prejudice the carrying out of social work because it would be likely to cause serious harm to the physical or mental health or condition of the individual or another person.

Information about physical or mental health condition.

The authority must not disclose this kind of information to the service user or person requesting the file on behalf of the service user without first consulting an 'appropriate health professional'. This would normally be the person responsible for the individual's current clinical care in connection with matters to which the information relates.

Other legislation.

Where other legislation prevents disclosure, then the person cannot rely on the Data Protection Act 1998 to seek access to records. These include, for example, adoption records and reports; parental order records and reports. (Adoption Records are accessed through the Adoption Service; requests should be made directly to them).

Refusal to access.

If access is refused, this should be notified to the person requesting access as soon as practicable and in writing, even if the decision has also been given in person. The employee should record the reasons for the decision and explain these to the individual.

Formal access

This applies to requests for access made formally to Social Care settings in writing (or by fax or E-mail).
Service user and carers rights under the law

The Data Protection Act requires information to be recorded in an appropriate form. Copies of the information must be supplied if requested. However the Authority need not supply a copy if it is not possible, or would involve disproportionate effort, or if the individual agrees otherwise

Some of the material may be known to an individual, but it may still be helpful to have someone available to help the person 'take in' the material or explain anything that is not understood

The service user has the right to amend inaccurate information and to receive a copy of any such additions, amendments, deletions or notes. Where agreement on changes cannot be reached and they remain the same this must be recorded on the record

When a request for Access to Records is made this will apply to both manual and electronic files.

Third Party Information

Personal information may include details about another person (a third party). If disclosure would allow the third party to be identified the Access to Records Officer must confirm the third party's consent before disclosure. If it is reasonable in all the circumstances the information could be disclosed

To decide what is reasonable, the following factors must be considered:

- Any duty of confidentiality owed to the third party
- Any steps taken to seek their consent
- Whether the third party is capable of giving consent
- Whether consent has been expressly refused
- Any legal prohibition

If consent is not given by a third party within 40 days, PCC should give as much information as possible without identifying the third party and should give an explanation why some of the information requested has not been given.

Access to records procedure

Formal requests should be notified to the key worker / internal social worker who will be responsible for responding to any requests. An acknowledgement letter of the request and to ask for any further information required to identify the individual and locate the information should be sent within 5 working days.

Requests must be responded to within 40 days of receiving the request. The 40 day period does not start until the following information has been received:

- Any information reasonably required to identify the individual
- Any information reasonably required to locate the information

The key worker / internal social worker who has received the request is responsible for:

- Locating all the relevant information
- Arranging access to the files
- Arranging an appropriate person to accompany the individual whilst they are accessing their files
- Authenticating the identification of individuals before access
- Gaining third party consent of disclosure
- Ensuring that any third party information where consent is not agreed is removed or anonymised before access
- Replying within 40 days of receipt of the request for access
- Monitoring the progress of all requests
- Scanning the file before access to identify any third party information
- Scanning any 'privileged' information
- Removing any third party information where access has not been agreed
- If the personal information requested is not held, the key worker / internal social worker must inform the applicant as soon as possible.

Where an appointment has been made to see records and no response has been received from the applicant (or if the applicant does not keep the appointment) a second appointment will be offered. If this fails a new access request will have to be made.

In some cases it may be deemed appropriate to send a copy to the applicant in the post (for example, if they live too far away to travel to our registered offices). In these circumstances the applicant must be informed that it will be sent via recorded delivery and that they may wish to contact the office to discuss issues relating to the composition of their file once they have had the opportunity to read through it.

COMMUNICATIONS POLICY

INTRODUCTION

1) IT and Communication plays an essential role in the conduct of our business. The IT infrastructure including e-mail and internet access have therefore significantly improved business operations and efficiencies.

2) How you communicate with people not only reflects on you as an individual but also on us as a business. As a result of this the company values your ability to communicate with colleagues, clients/customers and business contacts but we must also ensure that such systems and access are managed correctly, not abused in how they are used or what they are used for.

3) This policy applies to all members of the Company who use our or our clients' communications facilities, whether Directors/Consultants, full or part-time employees, contract staff or temporary staff. The parameters and restrictions are outlined below and you are required to read them carefully.

GENERAL PRINCIPLES

1) You must use our and our clients' information technology and communications facilities sensibly, professionally, lawfully, consistently with your duties and in accordance with this policy and other Company rules and procedures.

2) At all times employees must behave with honesty and integrity and respect the rights and privacy of others in relation to electronic communication and information. The company reserves the right to maintain all electronic communication and files.

3) Every employee will be given access to the Intranet and/or Internet as appropriate to their job needs. For those who do not have daily PC access occasional access will be arranged, as necessary, by Management,

4) All PC/network access will be through passwords, and no individual is permitted onto the system using another employee's password. Employees are not permitted to share their password with anyone inside or outside the company. Individuals will be allowed to set their own passwords, and must change them as frequently as requested by the system set-up requirements.

5) All information relating to our clients/customers and our business operations is confidential. You must treat our paper-based and electronic information with utmost care.

6) Many aspects of communication are protected by intellectual property rights which can be infringed in a number of ways. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or of other intellectual property rights.

7) Particular care must be taken when using e-mail as a means of communication because all expressions of fact, intention and opinion in an e-mail may bind you and/or the Company and can be produced in court in the same way as other kinds of written statements.

8) If you are speaking with someone face to face, via the telephone, in writing via whatever medium you are a representative of the Company. Whilst in this role you should not express any personal opinion that you know or suspect might be contrary to the opinions of the Directors or Company policy.

9) You must not use any of our or our clients' media to do or say anything which would be subject to disciplinary or legal action in any other context such as sending any sexist, racist, defamatory or other unlawful material. If you are in doubt about a course of action, take advice from a member of management.

USE OF ELECTRONIC MAIL

1) **Business use**

Always use the "Bcc" box when mailing to groups whenever the members of the group are unaware of the identity of all the others (as in the case of marketing mailing lists), or where you judge that the membership of the group of one or more individuals should perhaps not be disclosed to the others (as in the case of members of a staff benefit scheme), because if you use the "Cc" box each recipient is informed of the identity (and in the case of external recipients, the address) of all the others. Such a disclosure may breach any duty of confidence owed to each recipient, breach the Company's obligations under the General Data Protection Regulation and Data Protection Act or may inadvertently disclose confidential business information such as a marketing list. This applies to both external and internal e-mail.

Expressly agree with the customer/client that the use of e-mail is an acceptable form of communication bearing in mind that if the material is confidential, privileged or commercially sensitive then un-encrypted e-mail is not secure.

If you have sent an important document, always telephone to confirm that the e-mail has been received and read.

In light of the security risks inherent in web-based e-mail accounts, you must not e-mail business documents to your personal web-based accounts. You may send documents to a customer's/client's web-based account if you have the customer's/client's express written permission to do so. However, under no circumstances should you send sensitive or highly confidential documents to a customer's/client's personal web-based e-mail account (e.g. Yahoo, or Hotmail), even if the customer/client asks you to do so.

Personal use

a) Although our e-mail facilities are provided for the purposes of our business, we accept that you may occasionally want to use them for your own personal purposes. This is permitted on condition that all the procedures and rules set out in this policy are complied with. Be aware, however, that if you choose to make use of our facilities for personal correspondence, the Company may need to monitor communications for the reasons shown below.

b) Under no circumstances may the Company's facilities be used in connection with the operation or management of any business other than that of the Company or a customer/client of the Company unless express permission has been obtained from a member of management.

c) You must ensure that your personal e-mail use:

- does not interfere with the performance of your duties;
- does not take priority over your work responsibilities;
- does not cause unwarranted expense or liability to be incurred by the Company or our clients;
- does not have a negative impact on our business in any way; and
- is lawful and complies with this policy.

d) The Company will not tolerate the use of the E-mail system for unofficial or inappropriate purposes, including:

(i) any messages that could constitute bullying, harassment or other detriment;

(ii) on-line gambling;

(iii) accessing or transmitting pornography;

(iv) transmitting copyright information and/or any software available to the user; or

(v) posting confidential information about other employees, the Company or its customers or suppliers.

USE OF INTERNET AND INTRANET

1) We trust you to use the internet sensibly. Although internet facilities are provided for the purposes of our business, we accept that you may occasionally want to use them for your own personal purposes. This is permitted on condition that all the procedures and rules set out in this policy are complied with and your use of the internet does not interfere in any way with the performance of your duties.

2) Whenever you access a web site, you should always comply with the terms and conditions governing its use. Care must be taken in the use of information accessed through the Internet. Most information is unregulated, and as such there is no guarantee of accuracy.

3) The use of the Internet to access and/or distribute any kind of offensive material, or material that is not work-related, leaves an individual liable to disciplinary action which could lead to dismissal.

4) You must not:

   a) use any images, text or material which are copyright-protected, other than in accordance with the terms of the license under which you were permitted to download them;

   b) introduce packet-sniffing or password-detecting software;

   c) seek to gain access to restricted areas of the Company's network;

   d) access or try to access data which you know or ought to know is confidential;

   e) introduce any form of computer virus; nor

   f) carry out any hacking activities.

VIRUS PROTECTION PROCEDURES

In order to prevent the introduction of virus contamination into the software system the following must be observed:-

   a) unauthorised software including public domain software, magazine cover disks/CDs or Internet/World Wide Web downloads must not be used; and

   b) all software must be virus checked using standard testing procedures before being used.

USE OF COMPUTER EQUIPMENT

In order to control the use of the Company's computer equipment and reduce the risk of contamination the following will apply:

   a) The introduction of new software must first of all be checked and authorised by a member of management or a client's nominated senior member of management before general use will be permitted.

   b) Only authorised staff should have access to the Company's computer equipment.

   c) Only authorised software may be used on any of the Company's computer equipment.

d) Only software that is used for business applications may be used.

e) No software may be brought onto or taken from the Company's premises without prior authorisation.

f) Unauthorised access to the computer facility will result in disciplinary action.

g) Unauthorised copying and/or removal of computer equipment/software will result in disciplinary action, such actions could lead to dismissal.

SYSTEM SECURITY

1) Security of our or our clients' IT systems is of paramount importance. We owe a duty to all of our customers/clients to ensure that all of our business transactions are kept confidential. If at any time we need to rely in court on any information which has been stored or processed using our IT systems it is essential that we are able to demonstrate the integrity of those systems. Every time you use the system you take responsibility for the security implications of what you are doing.

2) The Company's system or equipment must not be used in any way which may cause damage, or overloading or which may affect its performance or that of the internal or external network.

3) Keep all confidential information secure, use it only for the purposes intended and do not disclose it to any unauthorised third party.

WORKING REMOTELY

1) This part of the policy and the procedures in it apply to your use of our systems, to your use of our laptops, and also to your use of your own computer equipment or other computer equipment (e.g. client's equipment) whenever you are working on Company business away from our premises (working remotely).

2) When you are working remotely you must:

a) password protect any work which relates to our business so that no other person can access your work;

b) position yourself so that your work cannot be overlooked by any other person;

c) take reasonable precautions to safeguard the security of our laptop computers and any computer equipment on which you do Company business, and keep your passwords secret;

d) inform the police and the Company as soon as possible if either a Company laptop in your possession or any computer equipment on which you do our work has been stolen; and

e) ensure that any work which you do remotely is saved on the Company system or is transferred to our system as soon as reasonably practicable.

3) PDAs or similar hand-held devices are easily stolen and not very secure so you must password-protect access to any such devices used by you on which is stored any personal data of which the Company is a data controller or any information relating our business, our clients or their business.

PERSONAL TELEPHONE CALLS/ MOBILE PHONES

1) Telephones are essential for our business. Incoming/outgoing personal telephone calls are allowed at the Company's head office but should be kept to a minimum. We reserve the right to recharge for excessive personal use. When visiting or working on client premises you should always seek permission before using our clients' telephone facilities.

2) Personal mobile phones should be switched off or 'on silent' during working hours and only used during authorised breaks.

MONITORING OF COMMUNICATIONS BY THE COMPANY

1) The Company is ultimately responsible for all business communications but subject to that will, so far as possible and appropriate, respect your privacy and autonomy. The Company may monitor your business communications for reasons which include:

a) providing evidence of business transactions;

b) ensuring that our business procedures, policies and contracts with staff are adhered to;

c) complying with any legal obligations;

d) monitoring standards of service, staff performance, and for staff training;

e) preventing or detecting unauthorised use of our communications systems or criminal activities; and

f) maintaining the effective operation of Company communication systems.

2) From time to time the Company may monitor telephone, e-mail and internet traffic data (i.e. sender, receiver, subject; non-business attachments to e-mail, numbers called and duration of calls; domain names of web sites visited, duration of visits, and non-business files downloaded from the internet) at a network level (but covering both personal and business communications). This includes monitoring of any additional accounts you may be requested to set up for the purposes of performing your work tasks, which are subject to the same rules as your work email account. Information acquired through such monitoring may be used as evidence in disciplinary proceedings.

3) Sometimes it is necessary for us to access your business communications during your absence, such as when you are away because you are ill or while you are on holiday.

DATA PROTECTION

1) As an employee using our communications facilities, you will inevitably be involved in processing personal data for the Company as part of your job. Data protection is about the privacy of individuals, and is governed by the General Data Protection Regulation and current Data Protection Act.

2) Whenever and wherever you are processing personal data for the Company you must keep this secret, confidential and secure, and you must take particular care not to disclose such data to any other person (whether inside or outside the Company) unless authorised to do so. Do not use any such personal data except as authorised by us for the purposes of your job. If in doubt ask a member of management.

3) The Act gives every individual the right to see all the information which any data controller holds about them. Bear this in mind when recording personal opinions about someone, whether in an e-mail or otherwise. It is another reason why personal remarks and opinions made should be given responsibly, must be relevant and appropriate as well as accurate and justifiable.

4) For your information, the Act provides that it is a criminal offence to obtain or disclose personal data without the consent of the data controller. "Obtaining" here includes the gathering of personal data by employees at work without the authorisation of the employer. You may be committing this offence if without authority of the Company: you exceed your authority in collecting personal data; you access personal data held by us; or you pass them on to someone else (whether inside or outside the Company).

USE OF SOCIAL NETWORKING SITES

Any work related issue or material that could identify an individual who is a customer/client or work colleague, which could adversely affect the company a customer/client or our relationship with any customer/client must not be placed on a social networking site. This means that work related matters must not be placed on any such site at any time either during or outside of working hours and includes access via any computer equipment, mobile phone or PDA.

CONFIDENTIALITY

Employees are not permitted to register with sites or electronic services in the company's name without the prior permission of their manager. They are not permitted to reveal internal company information to any sites, be it confidential or otherwise, or comment on company matters, even if this is during after-hours or personal use. The company confidentiality policy applies to all electronic communication and data.

COMPLIANCE WITH THIS POLICY

Failure to comply with this policy may result in disciplinary action being taken against you. If there is anything in this policy that you do not understand, please discuss it with a member of management.

Please note that the procedures and policies outlined in this policy, and in any related policy, may be reviewed or changed at any time.

Confidentiality Policy

Scope

This policy applies to all PCC employees, including:

- Permanent staff
- Voluntary staff
- Placements and Work Experience
- Temporary staff

Purpose

The purpose of this policy is to detail the basic standards that PCC should adhere to, and which can be incorporated as part of normal working practice

Introduction

PCC is committed to fulfilling its duties and responsibilities in regard to the confidentiality of information that the agency receives, has access to and stores as outlined in:

- Foster Service Regulations 2011 (Section 22)
- Fostering Services: National Minimum Standards 2011 (Standard 26)
- The Data Protection Act 1998
- The Human Rights Act 1998

This policy should be seen as an integral part of ensuring that Phoenix Community Care provides a safe environment where staff and service users are treated with respect. To not put the staff and service user under any harm and to protect their personal lives

Statement on Confidentiality

PCC offers confidentiality. Any sensitive information given will not be passed on except in very rare circumstances where this is necessary to protect a person from harm, or to comply with the law. In such circumstances, the information will only be passed on as permitted in this policy.

This must be confirmed with the Directors and the Database Manager. Wherever possible and appropriate the person will be informed that this action has been taken.

Confidentiality in Practice

The vast majority of enquiries can be treated in strict confidence. It is not necessary to inform all enquirers of the confidentiality policy as a matter of course, as to do so may be off-putting to those simply seeking information.

However, should the enquirer ask about confidentiality, or indicate that they are about to disclose information of a sensitive and serious nature, they should be made aware of the policy statement on confidentiality. The following easy to read phone statement should be read out in these circumstances:

PCC offers a confidential service. This means that usually, anything you tell the person from PCC will be kept private. But sometimes I may have to 'break confidentiality' – this means telling someone in a position of authority. This is very rare. I only have to do this if someone is in danger, and needs help. I will only tell the people who need to know. Callers have the right to decide what information they choose to share with PCC. Cases should not be discussed in any out-of-work context, even when the enquirer cannot be identified.

No personal details of any member of staff, client or volunteer will be disclosed without their agreement.

Permission must be gained from PCC's Data Protection Officer or PCC's Database Administrator to ensure compliance before publishing case studies (e.g. for training or information materials). Alternatively, fabricated case studies may be used for these purposes, but in either case details must be sufficiently disguised that the original enquirer cannot be identified.

Informing service users of the confidentiality policy

Any user of the service can see a copy of the confidentiality policy and our privacy policy on the website and in the Members Forums at this url: http://www.phoenixcommunity.org/policies

Exceptions to confidentiality

The only exceptions to complete confidentiality are when:

- The enquirer describes a situation, which raises concerns about the safety of a child or adult.
- The enquirer is in immediate danger, e.g. suicidal; threats of harm etc.
- The enquirer discloses information about an alleged crime or discloses information that an alleged crime is going to happen.

In the case of concerns about a child or adult in immediate danger, or an enquirer who is in immediate danger themselves, the staff member must call the police by dialling 999 immediately.

In all other cases of concerns about children or adults, the staff member must contact the NSPCC helpline or their local safeguarding children's board and explain the information they have received and follow the advice they are given.

Person who will help you decide what course of action to take.

Any information about any crime or criminal activity must be passed on to the police. In an emergency situation, PCC should contact the police and then notify the Directors as soon as possible. In all other situation Directors should be notified first that an outside service will be contacted, giving details of the situation without identifying information unless absolutely necessary.

Unauthorised breaches of confidentiality

Staff Member who breach these guidelines by communication, dissemination or solicitation of non-essential and/or identifying information about current or former staff, volunteers, service users or enquirers in any way other than authorised above may be to PCC disciplinary procedures.

DATA BREACH NOTIFICATION POLICY

AIM

We are aware of the obligations placed on us by the General Data Protection Regulation (GDPR) in relation to processing data lawfully and to ensure it is kept securely.

One such obligation is to report a breach of personal data in certain circumstances and this policy sets out our position on reporting data breaches.

PERSONAL DATA BREACH

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed.

The following are examples of data breaches:

a) access by an unauthorised third party;
b) deliberate or accidental action (or inaction) by a data controller or data processor;
c) sending personal data to an incorrect recipient;
d) computing devices containing personal data being lost or stolen;
e) alteration of personal data without permission;
f) loss of availability of personal data.

INVESTIGATION INTO SUSPECTED BREACH

In the event that we become aware of a breach, or a potential breach, an investigation will be carried out. This investigation will be carried out by **Gareth Hawkes, Director,** who will make a decision over whether the breach is required to be notified to the Information Commissioner. A decision will also be made over whether the breach is such that the individual(s) must also be notified.

WHEN A BREACH WILL BE NOTIFIED TO THE INFORMATION COMMISSIONER

In accordance with the GDPR, we will undertake to notify the Information Commissioner of a breach which is likely to pose a risk to people's rights and freedoms. A risk to people's freedoms can include physical, material or non-material damage such as discrimination, identity theft or fraud, financial loss and damage to reputation.

Notification to the Information Commissioner will be done without undue delay and at the latest within 72 hours of discovery. If we are unable to report in full within this timescale, we will make an initial report to the Information Commissioner, and then provide a full report in more than one instalment if so required.

The following information will be provided when a breach is notified:

a) a description of the nature of the personal data breach including, where possible:

   i) the categories and approximate number of individuals concerned; and
   ii) the categories and approximate number of personal data records concerned

b) the name and contact details of the data protection officer, **Gareth Hawkes**, where more information can be obtained;
c) a description of the likely consequences of the personal data breach; and
d) a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

WHEN A BREACH WILL BE NOTIFIED TO THE INDIVIDUAL

In accordance with the GDPR, we will undertake to notify the individual whose data is the subject of a breach if there is a *high* risk to people's rights and freedoms. A high risk may be, for example, where there is an immediate threat of identity theft, or if special categories of data are disclosed online.

This notification will be made without undue delay and may, dependent on the circumstances, be made before the supervisory authority is notified.

The following information will be provided when a breach is notified to the affected individuals:

a) a description of the nature of the breach
b) the name and contact details of the data protection officer where more information can be obtained
c) a description of the likely consequences of the personal data breach and
d) a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

RECORD OF BREACHES

The Company records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under GDPR. It records the facts relating to the breach, its effects and the remedial action taken.

PCC Charity Supporters, donators and subscribers

As a registered charity, PCC welcomes supporters/friends of PCC, regular donators, single donators and those who wish to subscribe to PCC's newsletter and promotional material.

The volume of personal data is low-moderate.

The sensitivity of the data is low: the most sensitive data being an e-mail address;
The risk of data breach is small – primarily the accidental disclosure of names & e-mail addresses.

Overall impact: LOW

By Consent

People who are interested in, and wish to be kept informed of, the activities of PCC.

Subject to the person's consent, this may include information selected and forwarded by the Charity on activities relevant to those of the Charity by other organisations.
Note: this will not involve providing the person's personal data to another organisation.

The information collected may additionally contain details of any particular areas of interest about which the person wishes to be kept informed.

The information provided will be held and processed solely for the purpose of providing the information requested by the person

Legitimate Interest

Volunteers, Including Trustees

In order to be able to operate efficiently, effectively and economically, it is in the legitimate interests of the Charity to hold such personal information on its supporters, donators, volunteers and trustees and as such their data, of any kind, is covered by this data protection policy in its entirety.