EVERY PARENT & CHILD

CONFIDENTIALITY, INFORMATION SECURITY AND COMPUTER USE POLICY

CONTENTS

1. INTRODUCTION & POLICY STATEMENT

1.1. Every Parent & Child (hereafter known as EPC) is committed to maintaining high standards of confidentiality and information security in all aspects of its work. This policy sets out the standards expected by EPC from people accessing personal information about clients, staff or volunteers and using its IT resources and communications systems.

1.2. All employees/volunteers and others attached to EPC will sign a confidentiality and information security agreement (appendix A). This states that a copy of this policy has been seen, understood and will be adhered to at all times.

Who is covered by the Policy?

1.3. This Policy covers all individuals working at all levels and grades, including senior managers, officers, directors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff and volunteers (collectively referred to as staff in this Policy). Third parties who have access to EPC electronic communication systems and equipment are also required to comply with this Policy.

Breaches of the Policy

1.4. A breach of confidentiality or any of the policies set out in this document will be viewed seriously and could result in disciplinary action up to and including termination of employment. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether EPC's equipment or facilities are used for the purpose of committing the breach. Any member of staff suspected of committing a breach of this Policy is required to co-operate with EPC's investigation, which may involve handing over relevant passwords and login details.

Personnel responsible for implementing the Policy

1.5. All staff are responsible for the success of this Policy and should ensure that they take the time to read and understand it. Any breach of this policy should be reported to your line manager.

1.6. All managers have a specific responsibility for operating within the boundaries of this Policy, ensuring that all staff understand the standards of behaviour expected of them and taking action when behaviour falls below its requirement.

1.7. Questions regarding the content or application of this Policy should be directed to the HR Manager or to the CEO in the absence of the HR Manager..

2. CONFIDENTIALITY

2.1. All records or information about clients, staff or volunteers must be treated as strictly confidential. The general rule is that any information concerning an individual or the organisation should not be discussed with anyone except in an official and professional capacity. Information obtained about a client or any member of their family should be only be used in support of their case.

2.2. Information takes many forms and includes images, data stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on memory sticks or cd-rom or spoken in conversation or over the telephone.

Confidentiality standards:

2.3. Information will only ever be shared on a "need to know" basis with other members of the team and will not be passed on to a third party without the consent of the owner of the information, unless the information comes within the scope of Child Protection or Abuse of Vulnerable Adults legislation and guidelines.

2.4. When a Child Protection or Abuse of Vulnerable Adults issue is suspected this should be reported immediately to the Manager and a decision will be taken as to the appropriate course of action following EPC's Safeguarding Policy and Procedures.

2.5. You must always seek permission from the person concerned before discussing a case with another professional in another organisation.

2.6. The service user/member of staff/volunteer will be told what information is being held about them, why the information is being held and who it will be shared with.

2.7. The service user/member of staff/volunteer has the right to review the information held and have it corrected if inaccurate.

2.8. The information should be held securely and only for as long as necessary.

2.9. It is the responsibility of all individuals to ensure the accuracy of personal information and keep it up to date as far as possible.

2.10. If consent has been obtained to share information it is the responsibility of the person passing on the information to ensure disclosure only takes place on the terms agreed. It is important the terms agreed are fully explained and understood by the recipient.

3. SECURITY AND STORAGE OF INFORMATION

3.1. All information whether held in manual or electronic systems must be protected against unauthorised access, use and disclosure.

Security & storage guidance:

3.2. All paper records/information including Personnel records must be stored in a lockable cabinet, cupboard or drawer.

3.3. All records/information held on computer are subject to the provisions of the Data Protection Act 1998.

3.4. Passwords should not be shared, sites should not be left open and screens should not be located where unauthorised persons can view personal information.

3.5. Confidential files sent by post must be sent recorded delivery and all confidential items marked "Strictly Private and Confidential" for the attention of the designated individual.

3.6. If information is requested by telephone the identity of the caller must be verified.

3.7. Information being faxed must be sent to a verified number that is not accessible to the general public.

3.8. Clients' records can only be taken outside of the office with the permission of the senior case worker or chief executive.

3.9. Care must be taken with records taken outside of the office with permission to avoid loss or theft.

3.10. Records taken outside of the office with permission must be returned promptly.

3.11. Duplicate records should not be retained outside the office.

3.12. Clients should not be contacted from a staff member's personal email address as this could compromise the safety of clients' details and email addresses and contravene EPC's Data Protection regulations.

3.13. Records are normally kept for two years and then any printed material containing personal information should be shredded or disposed of as confidential waste.

4. USE OF EMAIL, INTERNET & SOCIAL MEDIA

4.1. EPC recognises that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media, such as Facebook, Twitter, blogs and wikis. However, employees' use of social media can pose risks to EPC's confidential and proprietary information and reputation, and can jeopardise EPC's compliance with legal obligations.

4.2. No volunteer, sessional worker or any person other than a member of staff shall use the internet without prior permission.

4.3. Staff may be required to remove internet postings which are deemed to constitute a breach of this Policy. Failure to comply with such a request may result in disciplinary action.

4.4. Personal use of the internet or social media is never permitted during working time or by means of EPC's computers, networks and other IT resources and communications systems. EPC recognise that employees may occasionally desire to use social media for personal activities at the office or by mean of EPC computers, networks and other IT resources and communications systems. EPC authorise such occasional use during rest breaks so long as it does not involve unprofessional or inappropriate content and does not interfere with your employment responsibilities or productivity. While using social media at work, circulating chain letters or other spam is never permitted. Circulating or posting commercial, personal, religious or political solicitations, or promotion of outside organisations unrelated to EPC's business are also prohibited.

Compliance with related Policies and Agreements

4.5. The internet, email facilities and social media should never be used in a way that breaches any of EPC's other Policies. If an internet post would breach any of EPC's Policies in another forum, it will also breach them in an online forum. For example, employees are prohibited from using social media to:

- take any steps that would damage the reputation of EPC or which may bring EPC into disrepute
- defame or disparage EPC or its affiliates, customers, clients, business partners, suppliers, vendors or other stakeholders
- harass or bully other staff in any way or breach EPC's Anti-harassment and Bullying Policy
- unlawfully discriminate against other staff or third parties or breach EPC's Equal Opportunity Policy
- breach EPC's Data Protection Policy (for example, never disclose personal information about a colleague online)
- breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements)

4.6. Staff should never provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to EPC and create legal liability for both the author of the reference and EPC.

Email use guidance:

4.7. Minimise the forwarding of e-mails that contain non-business material.

4.8. Check receipt of important messages with a telephone call.

4.9. Never divulge your password or account information to other users.

4.10. Be aware that the sarcasm, humour, abuse, or tone can easily be misunderstood in e-mails.

4.11. Avoid using currency punctuation in text-based e-mails. Use three-letter currency indicators instead (e.g. GBP, USD, EUR)

4.12. If possible, refer to files on any network-shared areas rather than include the files as an attachment.

4.13. Send e-mails to individuals rather than groups.

4.14. Compress large attachments, if possible, before sending. For example, zip files.

4.15. Ignore and delete chain e-mails.

4.16. Avoid subscription services and automatic information services unless there is a good business reason for subscribing.

4.17. Check the authenticity (for example, by telephone) of suspicious messages.

4.18. Carry out regular housekeeping on your mailbox. Delete all e-mails as soon as possible and ensure that there is only one copy of any attachment in your mailbox.

4.19. Keep the number of e-mails in your mailbox to a minimum.

4.20. Check your personal address book regularly and remove unwanted and incorrect entries.

4.21. Always check that the addressee names are correct and be particularly aware of personal or global address groups.

Internet Use Guidance:

4.22. No programmes will be downloaded without the permission of the HR & Finance Manager and without clearance from our IT support agency.

4.23. No programmes shall be downloaded to use as screen savers without prior permission or clearance from our IT support agency.

4.24. No photographs other than those for use by Every Parent & Child should be downloaded or printed.

4.25. No sites that are not work related should be opened including pornographic, sales, entertainment etc.

4.26. Anyone suspecting that there is a virus in the system should inform the HR & Finance Manager immediately.

Use of Social Media Guidance:

4.27. As well as complying with 4.5 and 4.6 staff should make it clear in social media postings that they are speaking on their own behalf. Write in the first person and use a personal e-mail address when communicating via social media.

4.28. Staff are personally responsible for what they communicate in social media. Remember that what you publish might be available to be read by the masses (including EPC itself, future employers and social acquaintances) for a long time. Keep this in mind before you post content.

4.29. If you disclose your affiliation as an employee of EPC, you must also state that your views do not represent those of your employer. You should also ensure that your profile and any content you post are consistent with the professional image you present to clients and colleagues.

4.30. Avoid posting comments about sensitive business-related topics, such as EPC's performance. Even if you make it clear that your views on such topics do not represent those of EPC, your comments could still damage EPC's reputation.

4.31. If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from making the communication until you discuss it with your manager.

4.32. If you see content in social media that disparages or reflects poorly on EPC or EPC's stakeholders, you should contact your manager. All staff are responsible for protecting EPC's business reputation.

4.33. You are not permitted to add business contacts made during the course of your employment to personal social networking accounts, such as Facebook accounts or LinkedIn accounts.

4.34. The contact details of business contacts made during the course of your employment are regarded as EPC's confidential information and as such you will be required to delete all such details from your personal social networking accounts such as Facebook accounts or LinkedIn accounts, on termination of employment.

4.35. Do not post anything related to your colleagues or our clients, volunteers, business partners, suppliers, vendors or other stakeholders without their written permission.

5. ACCESS TO INFORMATION

5.1. All service users/staff members/volunteers are entitled to access, at reasonable notice, all of the information that Every Parent & Child holds about them as individuals in line with the Subject Access provisions of the Data Protection Act. All requests to access or review files must be in writing. If the request is from an outside source permission to disclose will be required.

6. DATA PROTECTION STATEMENT – EPC MEMBERS OF STAFF

6.1. In entering into their contracts of employment, members of staff consent to EPC processing data about them as necessary for the proper administration of the employment relationship, both during and after their employment.

6.2. The data may include (but is not limited to) information about qualifications, race or ethnic origin, gender, disability, matters of discipline, criminal convictions, age and years of service, membership of a recognised trade union, pensionable pay or contributions, matters relating to mental or physical health (including dates of absence due to illness and the reason for the absence) and matters relating to pregnancy and maternity leave.

6.3. Such data may be processed for any legitimate reasons connected with employment by EPC including payment of salary, pension, sickness benefit or other payments due under the contract of employment, monitoring absence or sickness, training and development purposes, negotiations with trade union or staff representatives, redundancy and succession planning, curriculum planning and organisation and to comply with any statutory or other legal obligation binding on EPC. This may also include the publication of the employees name and contact details in EPC publications and on the EPC internal and external websites. Data may also be processed to ensure compliance with the Disability Discrimination Act and EPC's Equal Opportunities Policy and from time to time information is required to be

sent for the purposes of statistical analysis and use by central government departments and agencies.

6.4. EPC also undertakes monitoring of computer facilities (including e-mail and access to the internet) in order to ensure the effective operation of the central computer and network systems and for other legitimate purposes. Members of staff should refer to the Computer Usage Policy (as amended from time to time) for further information.

6.5. Personal data will be processed only in accordance with EPC's registration under the Data Protection Act.

7. STAFF MONITORING

7.1. The contents of EPC's IT resources and communications systems are EPC's property. Therefore, staff should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on EPC's electronic information and communication systems.

7.2. EPC reserve the right to monitor, intercept and review, without further notice, staff activities using EPC's resources and communications systems, including but not limited to social media postings and activities, to ensure that EPC rules are being complied with and for legitimate business purposes and you consent to such monitoring by your acknowledgement of this Policy and your use of such resources and systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other networking monitoring technologies.

7.3. EPC may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice.

7.4. Do not use EPC IT resources and communications systems for any matter that you wish to be kept private or confidential from EPC.

Other policies to reference:

Safeguarding Policy and procedures

SENDIASS confidentiality procedures

Computer usage policy

Reviewed on: January 2019

Next review date: January 2020

APPENDIX A - CONFIDENTIALITY AND INFORMATION SECURITY AGREEMENT

CONFIDENTIALITY, INFORMATION SECURITY AND COMPUTER USE AGREEMENT

This Policy does not form part of any employee's contract of employment and it may be amended at any time.

I have received a copy of the Confidentiality, Information Security and Computer Use Policy. I have read the policy, understand it and will conform to its contents.

Signature …….

Name in block capitals ……..

Date …….