DATA PROTECTION, DATA SECURITY AND SOCIAL MEDIA POLICY AND PROCEDURES

Document Control Panel			
File Reference Number		Data Protection-PP-01	
File Name		Data Protection, Data Security and Social Media Policy and Procedures	
Owner		Marketing, IT & Communications Manager	
Approver		Director of Service Delivery/CEO	
History			
Date	Author's Name	Changes	Approved by Name
01/08/2013	LE	Drafted new P&P	
09/08/2013			GW/PS
10/09/2013			Board of Trustees
24/06/2014	LE	Reviewed P&P and updated Section 6	
13/11/2014	LE	Reviewed & updated following merger	
		Approved	IS Trustee
20/01/2016	LE	Reviewed & updated	
09/02/2016		Approved	IS Trustee
Next Review Date		01/2017	

Printed copies of this document are not version controlled.

INDEX

1 This Policy and these Procedures arise from

1.1 The Adoption Support Agencies (England) and Adoption Agencies (Miscellaneous Amendments) Regulations 2005, (Regulations 14, 15 and 22), and the National Minimum Standards for Adoption Support (Standard 17).

1.2 PAC-UK is committed to carrying out and meeting in full the requirements of the Data Protection Act, 1998 (the "Act") in processing all personal data in connection with its work. Its staff and trustees are therefore required to familiarise themselves with the requirements of the Act and to ensure that these are fully met.

1.3 In line with the Data Protection Act 1998 principles, PAC-UK will ensure that personal data will:

- Be obtained fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specific and lawful purpose.
- Be adequate, relevant but not excessive.
- Be accurate and kept up to date.
- Not be held longer than necessary.
- Be processed* in accordance with the rights of data subjects.
- Be subject to appropriate security measures.
- Not to be transferred outside the European Economic Area (EEA).

*the definition of 'Processing' is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper based personal data as well as that kept on computer.

2 Introduction and aims of this policy

2.1 The Data Protection Act 1998 seeks to strike a balance between the rights of individuals and the sometimes competing interests of those (such as PAC-UK) with legitimate reasons for using and recording personal information. It gives individuals certain rights regarding personal information held about them and places obligations on those who process such information. For the purposes of the Act, PAC-UK is the Data Controller.

2.2 PAC-UK needs to keep certain information on its employees, volunteers, service users and trustees to carry out its day to day operations, to meet its objectives and to comply with legal obligations.

2.3 The organisation is committed to ensuring any personal data will be dealt with in line with the Data Protection Act 1998. To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

2.4 The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation.

2.5 This policy covers employed staff, sessional workers, trustees and volunteers.

3 Policy implementation

3.1 To meet our responsibilities staff, volunteers and trustees will:

- Ensure any personal data is collected in a fair and lawful way.
- Explain why it is needed at the start.
- Ensure that only the minimum amount of information needed is collected and used.
- Ensure the information used is up to date and accurate.
- Review the length of time information is held.
- Ensure it is kept safely.
- Ensure the rights people have in relation to their personal data can be exercised.

3.2 PAC-UK will ensure that:

- Everyone managing and handling personal information is trained to do so.

- Anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do.
- Any disclosure of personal data will be in line with our procedures.
- Queries about handling personal information will be dealt with swiftly and politely.
- Training and raising awareness about the Data Protection Act and how it is followed in this organisation will be part of every new employee's induction training programme.
- PAC-UK's Data Protection Policy will be reviewed annually and all PAC-UK employees will receive policy update notifications.

4 Individual responsibilities

4.1 All staff and volunteers have a duty to observe the requirements of the Act and the PAC-UK policy in relation to it.

4.2 Individuals who do not handle personal data as part of their normal work still have a responsibility to ensure that any personal data they see or hear goes no further. This includes personal data and any information extracted from such data. Unauthorised disclosure might occur e.g. by passing information over the telephone, communicating information on a computer print-out or even inadvertently by reading a computer screen.

5 Data security guidelines for all staff and volunteers

5.1 Do not leave information about individuals on your desk when you are not using it.

5.2 Ensure that filing cabinets are kept locked.

5.3 Do not leave personal data displayed on screen, do not leave your computer logged on and unattended.

5.4 Do not give your password to anyone and do not choose a password that is easy to guess.

5.5 Password-protect documents sent via email that contain sensitive personal data. Passwords for the protected documents must be communicated separately from the email that contains the data.

5.6 Never record anything that isn't relevant to the specified purpose. Do not "trawl" for information in case "it might be useful later".

5.7 If you are unable to verify whether something is factual either do not record it until you are able to do this or make it clear in the record that this has not been verified.

Save all your documents into the relevant folders on My Office Data. Do not save any documents in the 'My Documents' folder on your individual computer.

6 Data security measures taken by PAC-UK

PAC-UK will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure by:

6.1 Ensuring firewall and virus-checking and ant-spyware software are installed on all computers and servers.

6.2 Ensuring our operating system is set up to receive automatic updates.

6.3 Protecting our computers by downloading the latest security updates.

6.4 Only allowing our staff access to the information they need to do their job and not allowing them to share passwords.

6.5 Encrypting any personal information held electronically that would cause damage or distress if it were lost or stolen.

6.6 Taking daily back-ups of the information on our computer system to ensure all data can be recovered in the event of server failure.

6.7 Securely removing all personal information before disposing of old computers.

6.8 Encrypting or password protecting all confidential documents to be sent via email.

6.9 Ensuring all members of staff are fully competent in using key Microsoft Office functions

6.10 Ensuring all members of staff are fully competent in using key Microsoft Outlook functions and are trained in how to use blind carbon copy (bcc) and carbon copy (cc) when sending confidential emails. PAC-UK has produced customised 'How to' guides with screenshot instructions which can be accessed in Controlled Forms on My Office Data. This will form part of induction training for every new member of staff with existing staff receiving refresher training annually.

6.11 Instructing staff not to open spam emails, not even to unsubscribe.

6.12 Shredding or collecting in specially marked bags all our confidential waste paper which is then collected and disposed of securely.

6.13 Checking the physical security of our premises in line with PAC-UK's H&S P&P's.

6.14 Training all new staff on Data Protection as part of their induction, reviewing our Data Protection Policy annually and distributing updated versions to all staff.

6.15 Using strong passwords for staff login accounts (incl. tablet devices) which have at least six characters and use a combination of upper/lower case letters, numbers and symbols.

6.16 Sending all confidential mail via Royal Mail Special Delivery (signed) when emailing confidential documents is not viable and including our return address on back of all mail so it can be returned safely if undeliverable.

6.17 Reviewing every hard copy active file at least annually to ensure that the information kept on it is that which is necessary for PAC-UK to carry out its legitimate functions; adequate, relevant and not excessive; accurate and up to date; not kept any longer than is absolutely necessary (subject to any statutory requirements in relation to the retention of records).

6.18 Any unauthorised disclosure of personal data to a third party by an employee may result in disciplinary procedures.

6.19 The Board and trustees are accountable for compliance of this policy. A trustee could be personally liable for any penalty arising from a breach that they have made.

6.20 Any unauthorised disclosure made by a volunteer may result in the termination of the volunteering agreement.

7 Type of information processed

7.1 **Personal data** means data which relates to a living individual who can be identified:

(a) From that data, or

(b) From that data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

It is important to note that, where the ability to identify an individual depends partly on the data held and partly on other information (not necessarily data), the data held will still be "personal data".

7.2 The Court of Appeal, in a recent case, concluded that data will relate to an individual if it "is information that affects (a person's) privacy, whether in his personal or family life, business or professional capacity".

7.3 The Court identified two notions that may assist in determining whether information "affects (an individual's) privacy" and therefore "relates to" an individual:

1. The first is whether the information is biographical in a significant sense; that is beyond the recording of (the individual's) involvement in a matter or an event which has no personal connotations.

2. The second concerns focus. The information should have (the individual) as its focus rather than some other person with whom he may have been involved or some transaction or event in which he may have figured or have had an interest.

7.4 The definition of what is personal data was extended by the Freedom of Information Act 2000, but this relates to the duties of statutory agencies or to voluntary agencies which are carrying out such duties on behalf of a statutory agency.

7.5 Specific provision is made under the Act for processing **sensitive personal data**. In the Act "sensitive personal data" means personal data consisting of information as to:

a) The racial or ethnic origin of the data subject

b) His/her political opinions

c) His/her religious beliefs or other beliefs of a similar nature

d) Whether he/she is a member of a trade union (within the meaning of the M1Trade Union and Labour Relations (Consolidation) Act 1992)

e) His/her physical or mental health or condition

f) His/her sexual life

g) The commission or alleged commission by him of any offence, or

h) Any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings

For personal information of this nature to be considered fairly processed, at least one of a number of extra conditions must be met (see Section 10)

8 Recording systems covered

Under the Act, the following recording systems are covered:

8.1 Information about an individual which is held or processed on computer (including emails) i.e. any equipment which operates automatically

8.2 Information about an individual which is kept in "relevant" manual files, i.e. "relevant filing systems"

8.3 Information about an individual which is intended to become part of one of these systems

8.4 In relation to manual files/records, the Court of Appeal concluded that: "a relevant filing system" for the purposes of the Act, is limited to a system:

In which the files forming part of it are structured or referenced in such a way as to clearly indicate at the outset of the search whether specific information capable of amounting to personal data of an individual requesting it is held within the system and, if so, in which file or files it is held; and

Which has, as part of its own structure or referencing mechanism, a sufficiently sophisticated and detailed means of readily indicating whether and where in an individual file or files specific criteria or information about the applicant can be readily located"

8.5 The 1998 Act more explicitly (than the 1994 Act) also includes non-text data such as photographs, audio and video material and biometric data (such as fingerprints, iris patterns or DNA samples) if these relate to identifiable living people.

9 The eight principles of good practice

9.1 The Act defines eight data protection principles of good practice:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-

   (a) At least one of the conditions in Schedule 2 is met, and

   (b) In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. About the rights of individuals e.g. personal data shall be processed in accordance with the rights of data subjects (individuals).

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

10 Conditions relevant to the first principle (schedule 2)

10.1 Personal data should only be processed fairly and lawfully. In order for data to be classed as 'fairly processed', at least one of these six conditions must be applicable to that data (Schedule 2):

1. The data subject (the person whose data is stored) has consented ("given their permission") to the processing;
2. Processing is necessary for the performance of, or commencing of, a contract;
3. Processing is required under a legal obligation (other than one stated in the contract);
4. Processing is necessary to protect the vital interests of the data subject;
5. Processing is necessary to carry out any public functions;
6. Processing is necessary in order to pursue the legitimate interests of the "data controller" or "third parties" (unless it could unjustifiably prejudice the interests of the data subject).

11 Conditions for processing sensitive personal data (schedule 3)

11.1 At least one of the above conditions must be met whenever you process personal data. However, if the information is sensitive personal data, at least one of several other conditions must also be met before the processing can comply with the first data protection principle. These other conditions are as follows:

- The individual who the sensitive personal data is about has given explicit consent to the processing.
- The processing is necessary so that you can comply with employment law.
- The processing is necessary to protect the vital interests of:
    - The individual (in a case where the individual's consent cannot be given or reasonably obtained), or
    - Another person, (in a case where the individual's consent has been unreasonably withheld).

- The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. Extra limitations apply to this condition.
- The individual has deliberately made the information public.
- The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights.
- The processing is necessary for administering justice, or for exercising statutory or governmental functions.
- The processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality.
- The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.

11.2 In addition to the above conditions – which are all set out in the Data Protection Act itself – regulations set out several other conditions for processing sensitive personal data; Their effect is to permit the processing of sensitive personal data for a range of other purposes – typically those that are in the substantial public interest, and which must necessarily be carried out without the explicit consent of the individual. Examples of such purposes include preventing or detecting crime and protecting the public against malpractice or maladministration. A full list of the additional conditions for processing is set out in the Data Protection (Processing of Sensitive Personal Data) Order 2000 and subsequent orders.

12 PAC-UK's procedures for dealing with the processing of information, data and case records

12.1 PAC-UK is fully committed to complying with the eight principles (Section 9 of its Data Protection Policy) regarding the processing of information which it holds in relation to its objectives.

12.2 In terms of the six conditions (Section 10) it is the policy of PAC-UK that data should normally only be processed with the full knowledge and consent of the Data Subject.

12.3 In any situation where it is proposed to record information without the consent of the data subject, the circumstances must be discussed and agreed with the line manager before this takes place. In the absence of the line manager, another line manager or the CEO should be consulted. If for any reason this is impossible, a line manager must be informed as soon as possible after the recording has taken place and the reasons why their prior agreement couldn't be obtained. The CEO must also be informed of all such circumstances.

12.4 Where this is agreed, a full note of the discussion and reasons for the decision will be placed in a prominent position in the front of the file. This note must be signed by the worker and countersigned by their line manager.

12.5 In the case of sensitive personal data, in order to comply with the additional conditions relating to such data (Section 11), the consent needs to be in writing and signed by the individual (subject), a copy of which will be retained on the file. The consent form must also state clearly the nature and purpose of the recording before it is signed by the individual. In any situation where it is proposed to record sensitive information without the explicit written consent of the individual concerned, the same procedure will be followed as that relating to non-sensitive personal data (1.2 and 1.3 above).

12.6 In order to comply with any other of the eight principles (Section 9), every active file will be reviewed at least annually to ensure that the information kept on it is:

- Only that which is necessary for the PAC-UK to carry out its legitimate functions
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept any longer than is absolutely necessary (subject to any statutory requirements in relation to the retention of records)

12.7 In terms of any non-current records, these will also be reviewed at least annually to ensure that any information recorded therein complies with each of these Principles. Only files which require to be kept in order to meet statutory requirements will be retained longer than 10 years unless there are deemed to be exceptional reasons, which will be recorded in writing on the file with a timescale set, beyond which the file will not be retained.

12.8 All personal records/data will be kept in locked cabinets/rooms, access to which is governed by PAC-UK's policy in relation to access to such records.

13 The rights of Data Subjects

13.1 Data Subjects have seven rights under the Data Protection Act:

1. The right to subject access:
   This allows an individual to find out what information is held about them on computer and some manual records.

2. The right to prevent processing:
   Anyone can ask a data controller not to process information relating to him/her that causes substantial unwarranted damage or distress to anyone else.

3. The right to prevent processing for direct marketing:
   Anyone can ask a data controller not to process information relating to him/her for direct marketing purposes.

4. Rights in relation to automated decision-taking:
   Individuals have a right to object to decisions made only by automatic means e.g. there is no human involvement.

5. The right to compensation:
   An individual can claim compensation from a data controller for damage and distress caused by any breach of the Act. Compensation for distress alone can only be claimed in limited circumstances.

6. The right to rectification, blocking, erasure and destruction:
   Individuals can apply to the court to order a data controller to rectify, block or destroy personal details if they are inaccurate or contain expressions of opinion based on inaccurate information.

7. The right to ask the Information Commissioner to assess whether the Act has been contravened:
   If someone believes their information has not been processed in accordance with the Data Protection Act, 1998 they can ask the Commissioner to make an assessment. If the Act is found to have been breached and the matter cannot be settled informally, an enforcement notice may be served on the data controller concerned.

Any individual has the right to appeal to the Information Commissioner or to take action through the Courts to seek a remedy where any of the rights 1-6 above have not been upheld or where s/he is unhappy or dissatisfied with the outcome.

14 Subject access requests

14.1 Subject to a limited number of exceptions made under Part IV of the Act or provided for by other (e.g. adoption) legislation, any living person who is the subject of personal information held and processed by PAC-UK has a right of access to that data. This information includes factual information, expressions of opinion and any intentions of PAC-UK in relation to the individual. Where access is refused, they may appeal to the courts or to the Information Commissioner.

NOTE: The exceptions under Part IV of the Act relate to statutory agencies unless either an organisation has been designated by the Secretary of State for Health or is essentially carrying out local authority social work functions.

Otherwise, access can be denied to:

- Any confidential reference PAC-UK has sent (but not those received),
- Any information used for "management forecasting or planning" if this would "prejudice the conduct" of PAC-UK's business

- Details of the organisation's intentions in negotiations if this would ruin its bargaining position - material subject to legal privilege

14.2 A person does not have the right to know what is recorded about anyone else. Thus, if a "family" file has been maintained, the individual does not have the right to see information about another family member without their consent. However, there may be circumstances in which the agency considers it reasonable to disclose information without consent (see Sections 3.4 and 3.8).

14.3 Where disclosure of information is not possible without disclosing information about another person, normally the request need not be complied with unless the other person has given consent to the disclosure. However, as much of the information sought as can be disclosed without revealing the other person's identity (whether by omission of names or other identifying particulars) must be provided.

14.4 There may be situations where it is considered to be "reasonable in all the circumstances" to comply with the request without the other person's consent. This includes the disclosure of identifiable information about a "source" who has contributed to the record. In determining what is "reasonable in all the circumstances", it is necessary to have regard to:

- Any duty of confidentiality owed to that other person
- Any steps taken with a view to seeking the consent of the other person to the disclosure
- Whether the other person is capable of giving consent
- Any express refusal of consent by the other person

Special considerations apply where the request is:

- By or on behalf of a child or young person under 18
- Made on behalf of an adult lacking mental capacity
- Made through another person (an agent)

14.5 The Data Protection Act only applies to data about living persons. Therefore any records relating to someone who has died is not personal data in accordance with the Act. Nevertheless, there may still be issues of confidentiality in relation to access to records about them.

15 PAC-UK's Policies and Procedures for dealing with requests for access

15.1 Any requests for access need to be referred to your line manager for consideration. Where it is concluded by the line manager in consultation with the worker that access should not be allowed, the request together with the reasons for this must be referred to the CEO for a final decision.

15.2 A fee of £10.00 will be charged for processing any request for access, although this may be waived where there are felt to be compelling reasons for this. The applicant should be informed of the fee payable and PAC-UK is not required to provide the information requested or process the application until the fee has been received.

15.3 It is vital that the identity of the applicant is satisfied beyond all reasonable doubt to ensure that information is not passed to someone who is not entitled to receive it. It is also important to clarify at the outset exactly what information is being requested. PAC-UK is not required to respond unless/until it is satisfied about the applicant's identity and the information requested.

15.4 Access can also be refused where PAC-UK has complied with a similar or identical request from the same individual, unless a reasonable period has elapsed since then. The nature of the information, the purpose for which it is processed and the frequency with which it is altered are all matters which should be considered in determining what is a "reasonable period".

15.5 Responses to requests for access must be made within 40 days of receipt of the request and the fee.

15.6 The information to be provided is all the data held about the data subject at the time that the request is received, unless it is subject to any exemptions or another person has refused to consent to disclosure of data identifying them. It should not be altered in order to make it acceptable to the applicant. Any amendment or deletion made between the request being received and complied with may be taken into account provided these would have been made whether or not a request had been received.

15.7 The Data Protection Act requires the information to be communicated in an intelligible form and that the applicant to be provided with a permanent copy of the information. However, PAC-UK is not obliged to supply a copy if it is not possible, or would involve disproportionate effort, or the applicant agrees otherwise (e.g. where s/he wants only an extract from a lengthy file). A worker should be made available to help the applicant to absorb the information and to clarify anything that s/he doesn't understand.

15.8 Where the information requested will include information about another person which would allow him/her to be identified, normal practice in PAC-UK is to seek his/her consent before releasing the information. If it is felt it is reasonable in all the circumstances that the information should still be supplied without the consent of the other person(s) this should be discussed and agreed with your line manager and the circumstances reported to the CEO. This is likely to be particularly applicable where the request relates to very old files and the possibility of tracing other identified persons is considered to be remote.

NOTE: PAC-UK may later be required to justify its actions if it supplies identifying information without the consent of the other person(s) and s/he/they later claim that the disclosure was a breach of their rights.

16 The right to rectification, blocking, erasure and destruction and PAC-UK's Policies and Procedures in relation to such requests

16.1 If an individual considers that any personal information held by the PAC-UK about him/her is inaccurate in any way s/he has the right to request that it should be rectified, blocked, erased or destroyed.

"Inaccurate" means incorrect or misleading in any matter of fact. A statement of opinion need not be corrected or erased unless it appears to have been based on an inaccurate fact.

16.2 PAC-UK's Policies and Procedures in relation to such requests:

- All such requests must be dealt with promptly in order to avoid a court action or intervention by the Information Commissioner. Although the Act does not specify a timescale for this, the Department of Health Guidance suggests that a response should be made within 21 days and this is the timescale which the PAC-UK has adopted for a response to be made.
- Whenever such a request is received, this must be discussed with your line manager and a conclusion reached. Where it is decided to accede to the request, the necessary action should be taken. The applicant should be informed accordingly and a copy of the corrected data supplied to him/her.
- (A note of this and the action taken also needs to be passed to the CEO).
- In all situations where it is decided not to agree, the request must be referred to the CEO for further consideration, together with the original reasons for not agreeing to this. Any decision not to accede to such a request will only be made by the CEO who will then inform the applicant and give reasons for this.

- If it is not accepted that the data is inaccurate, it must be noted on the file that the subject regards the information as inaccurate.

16.3 If the applicant is dissatisfied with the response s/he can:

- Approach the Information Commissioner, or
- Apply to the courts for an order requiring the data to be rectified, blocked, erased or destroyed

16.4 If the Commissioner or the courts uphold the subject's request, PAC-UK may be ordered to correct the data and may also be required to inform other organisations who have received the information of the correction. Compensation may also be awarded for any damage suffered as a result of the data requiring rectification.

17 Annual reporting

17.1 A report will be made to the Trustees annually by the CEO, of PAC-UK's compliance with the requirements of the Data Protection Act, 1998. This will include brief details of all situations where consent has not been obtained to processing (1, 2, 3 and 4 above); of compliance with the other Principles and of all situations in which requests have been received from data subjects for access to their records or that these should be rectified. Brief details will be included of all situations in which access has been refused or where rectification has not been carried out together with details of any further action taken by the subjects (through the Information Commissioner or the courts) and the outcomes.

18 PAC-UK's social media rules

18.1 The term Social Media refers to a number of websites and internet media resources which enable users to share information, opinions and social exchanges.

They are normally free to use, are unregulated except by the users themselves, and can be used or looked at by anyone with internet access, anywhere in the world. Examples of social media are blogs, social networking sites (e.g. Facebook and Twitter), podcasts, message boards and chat rooms.

18.2 We recognise that employees will use these media outside work, and they can be usefully used within work to make business contacts, exchange ideas and views about products and issues, and improve customer service.

18.3 Because of the global nature of the media and its potential, some rules need to be devised to ensure the media are used safely and effectively, and these are set out below:

a) You may only login to the backend of PAC-UK's social media streams and make posts on behalf of PAC-UK if approved by PAC-UK's CEO.

b) You may not share any information which is commercially sensitive, private or copyrighted.

c) You must comply with any other guidance we give from time to time concerning use of social media.

d) Be wary of any potential issues concerning information exchanged, such as defamation, breach of privacy and copyright, and comply with the law at all times.

e) You must not identify or refer to any clients, ex-clients or prospects.

f) Be yourself and do not use separate identities or pseudonyms online. If you are on a business related site such as a professional body or business forum, and you think it is appropriate, you may identify yourself with your job title and give the name of your employer. However, you are not speaking on PAC-UK's behalf and if necessary you should state that any views expressed are your own.

g) Use common sense. Apply your judgment and exercise discretion. Respect your audience as you cannot know who is reading your posts. Do not make any derogatory personal comments or offensive remarks. Be mindful that anything you publish is instantly available worldwide and for a long time in the future. It cannot be retracted and you are personally responsible for it.

h) Protect your own privacy and do not disclose any personal information.

19 Review

19.1 This policy will be reviewed annually to ensure it remains up to date and compliant with the law.