Digital communication procedures and confidential data security guidelines

At Triple A we regularly handle confidential data and communications. We have a legal obligation to handle this information securely and prevent unauthorised access to this information. These guidelines should help you do this but they aren't an exhaustive list. As a Triple A employee, or subcontractor, you have the responsibility to maintain alertness around potential risks to data security. These procedures are a starting point:

1. When sending emails to more than one service user, or member of public, at once, always use BCC to avoid giving their contact details to other service users. Use sensible discretion when sharing professional's contact information with other professionals. If in doubt, always ask their permission.

2. If sharing service user details with another professional. Always ensure you have the service user's permission, unless you have genuine concerns that they me be at serious risk of harm or of harming others. Some service users consent to information sharing with certain services on referral, you can check this on their referral form.

3. Do not send client related documents as email attachments if you can avoid it, you can share access to documents directly to email addresses within Triple A. Where you cannot avoid it, you must password protect the document and communicate the password to the recipient in a separate email, then delete the password email from your outbox and ask the recipient to store it securely then delete your email.

4. Do not use client names in email subject bars, use initials only.

5. If you need to seek guidance about a client with another professional and you have not obtained permission from the client to disclose their details, describe the situation to the professional without disclosing the client name or any identifying details. It may be necessary to do this if, for example, you wish to seek the advice of the safeguarding team before you decide whether an individual's situation meets the referral threshold.

6. If you think there may have been a data breach, accidental or otherwise, don't panic, inform a member of the senior management team immediately and they will take you through next steps.

7. Ensure any phone calls where service user details might be disclosed are made in a private place where they cannot be overheard.

8. Do not store client paperwork offline or on your personal one-drive. Ensure all client paperwork is kept on Triple A's shared OneDrive and is saved in a folder with the correct access permissions e.g. Named Navigator folders are only accessible by the named Navigator, management and admin.

9. Sometimes clients are mentioned or discussed during all-staff meetings, this should be done using initials only.

10. It is important to document all incidents and challenges involving service users in the appropriate place e.g. contact log, incident form. It should be borne in mind, however, that service users have a right to make a freedom of information request to view any documentation pertaining to them. You should therefore always use respectful language when writing up client notes and incidents. If you need to mention another individual in client notes, do this only by initial or relationship to client e.g. "client's Mum".

11. Do not click on any links in emails unless you are certain they are genuine. If you are at all unsure, forward these to support@davidallen-it.co.ukto check.

12. There are some times when it is OK to disclose client details without their consent, to risk holding organisations e.g. police, social services or other emergency services, where you fear they may be a risk to themselves or others. Their GP is also someone you can share legitimate concerns for their wellbeing with, without their permission. You should always check with the on call manager first, unless the risk is immediate and obtain the client's permission wherever possible.

13. Ensure all work phones, laptops or other IT equipment are either kept with you or stored securely and do not make a not of your passwords anywhere where they may be found.
14. Do not use physical notebooks or paper to write down client notes or details and do not print out digital versions. If you feel you may need to do this as an accommodation, discuss this with your supervisor and they will help you devise a way of doing so securely.