Related Documents

The Data Protection Act 2018 (UK's implementation of the General Data Protection Regulation (GDPR)).
FQ002 Incident Report form
FQ003 Confidentiality Notice Information Sharing Consent
PQ 015 Incident Reporting Policy
FQ008 Confidentiality and Data Protection Statement for Volunteers
FQ008a Privacy Notice – Data Protection
FQ008c Confidentiality Agreement Employee and Contractor
PQ18a Computer and Mobile Device Policy
PQ018c Personal Data Breaches
FQ038a Limitations of Use Statement

Scope

This policy applies to all Acacia Trustees, employees, volunteers and contactors.

Purpose

This policy highlights some key issues around information privacy and data protection that Acacia staff/volunteers/suppliers/visitors must be aware of. It is important to remember that our clients have trusted us with their sensitive and personal information and we need to take our obligations seriously to protect this information as part of our ambition to care for them. It is therefore vitally important that all staff, volunteers and others who handle personal information are familiar with, and comply with, this policy.

GDPR and the Data Protection Act both became law in May 2018. The primary aim of this data protection legislation is to give all individuals (expressed as 'data subjects' within the law) more control of personal data. It is about giving enhanced rights to individuals to find out about how their personal data is being used and recompense them if their personal data is being misused.

It is all about accountability and transparency and making sure that organisations that handle personal data are open and clear about how an individual's data is going to be used, and serious about the security of that data.

Acacia welcomes the new legislation. We are committed to keeping our client's, staff and volunteers safe. One of the ways we will do this is by respecting their personal information at all times, by being transparent, and doing our best to keep all personal information safe and secure.

Policy

1 Introduction

This policy identifies how Acacia Family Support (Acacia) executes its duty to keep personal information safe and confidential and compliant with data protection legislation. At the same time, not compromising its ability to deliver an effective support service for our clients and share information where it is needed. ***This policy must be read in conjunction with PQ18a Computer and Mobile Device Policy.***

Acacia will have full regard for current and future legal requirements which impinge on the confidentiality of:

- Personal information in general, and
- Specific/Special categories of personal information.

The Operations Director, Rob Ewers, is the data protection manager and takes responsibility for Acacia's ongoing compliance with this policy. Acacia is registered with ICO as an organisation which processes personal and special category data. This policy with be reviewed annually

2 Principles

2.1. The General Data Protection Regulation (GDPR) and Data Protection Act outlines six data protection principles that organisations need to follow when collecting, processing and storing individuals' personal data. The data controller is responsible for complying with the principles and must be able to demonstrate the organisation's compliance practices:

2.2. Lawfulness, fairness and transparency
The first principle is relatively self-evident: organisations need to make sure their data collection practices don't break the law and that they aren't hiding anything from data subjects.

2.3. Purpose limitation
Organisations should only collect personal data for a specific purpose, clearly state what that purpose is, and only collect data for as long as necessary to complete that purpose.

2.4. Data minimisation
Organisations must only process the personal data that they need to achieve its processing purposes.

2.5. Accuracy
The accuracy of personal data is integral to data protection. The GDPR states that "every reasonable step must be taken" to erase or rectify data that is inaccurate or incomplete. Individuals have the right to request that inaccurate or incomplete data be erased or rectified within 30 days.

2.6. Storage limitation
Similarly, organisations need to delete personal data when it's no longer necessary.

2.7. Integrity and confidentiality
This is the only principle that deals explicitly with security. The GDPR states that personal data must be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

In order to implement and properly maintain a robust information security function, Acacia recognises the importance of:

2.8. Understanding Acacia's information security requirements and the need to establish policy and objectives for information security;

2.9. Implementing and operating controls to manage Acacia's information security risks in the context of overall business risks.

2.10. Developing a culture of information security including regular training.

3. Legal Basis for collection and processing of personal information

3.1. The Acacia support service relies on the collection of core client data including personal identifying information, demographic data including special category data, assessment, risk management, care planning/delivery and progress reports. This combined data forms the health record for the client and is central to our ability to deliver an effective and safe support service for our clients whilst fulfilling our contractual and legal obligations as a health service provider.

3.2. The information which forms the health record is collected, stored and processed with legitimate interest as a legal basis.

3.3 Therefore it is not possible for the client to enter the service whilst withholding consent for the collection, storage and processing of their health record data. These two aspects are inextricably linked. Acacia has a legitimate interest in the processing and storage of personal information to deliver the service and where the client does not want this information stored/processed we are unable to offer a service.

3.4. Acacia recognises The Records Management Code of Practice for Health and Social Care (IGA, 2016) as the basis of our health records management procedures. Health records are therefore kept for 8 years in line with this guidance.

3.5. HR personal information is collected and processed on the basis of employment contract, legal obligation and legitimate interest. It is stored and processed for the periods defined by employment law. A copy of these data storage periods is available from the Business Support Officer.

3.6. Volunteer information is gathered and processed as part of the volunteer recruitment, placement, management and support practices. The information is held and processed with legitimate interests as our legal basis.

3.7. All personal information from clients, staff and volunteers obtained, stored and processed by Acacia for the purpose of promotion and marketing must only be done with the individuals specific consent as a legal basis.

4. Informed Consent

4.1. All staff and volunteers must be aware of the information contained in the appropriate privacy notice. The privacy notices (Client - FQ 018b, Staff - FQ 018c, Volunteers - FQ 018d) must be given to the individual prior to them providing us with their personal data. This notice should be sent to all clients prior to their initial telephone assessment. The privacy notice forms part of the resource pack which is sent to all clients prior to their first telephone assessment.

4.2. The personal information must only be used for the purpose it was given. If at some later point we decide that we would like to use it for a different purpose we must advise the individual of this re-purposing and obtain their consent (where we are to rely on consent as our legal basis for processing) unless there is another overriding legal basis for processing eg. court order.

4.3. Where it is proposed, in exceptional circumstances, that information about an individual should be shared with another agency or person, the consent of the individual, or the person who provided the information, should normally be sought.

4.2. This should be done in such a way that those persons know exactly what information will be passed on, to whom and for what purpose.

4.3. Information, which is confidential and restricted, will only be passed on where there is a clear need to know and where the expressed and informed consent has been obtained from the person whose information needs to be passed on.

4.4 The only exception to this is where there is imminent risk to the individual or someone else and/or significant safeguarding concern requiring referral. Please see FQ003 Confidentiality Notice Information Sharing Consent.

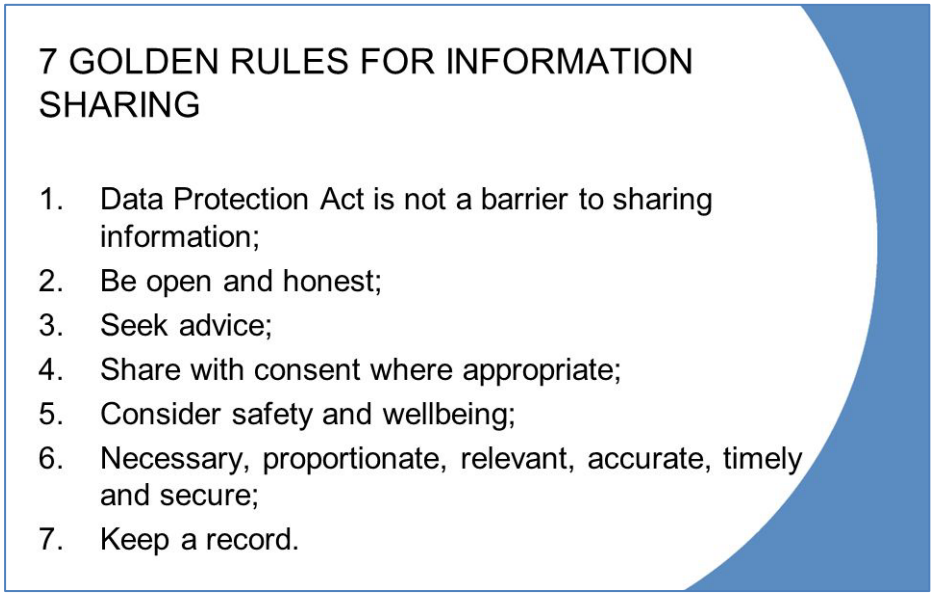
4.5. Wherever possible informed consent should be recorded in writing as a form of contract which gives the agreed terms and conditions of passing on and storing this information. When informed consent is being obtained on the telephone as part of an assessment/befriending session client consent should be recorded in the client management system. Written consent should then be obtained at the first face to face meeting or as soon as practically possible. This should be obtained using FQ003 Confidentiality Notice Information Sharing Consent.

4.7. The privacy notice must be given to the client before they enter the service. This document explains that legitimate interests is the legal basis for processing their personal information. The processing of this information is essential with regard to our ability to deliver a competent support service and comply with legal and contractual obligations regarding their health data. We cannot deliver a service without this information. The privacy notice is prominently displayed on our website and those who use our secure online referral forms are directed to it before referral. The notice is also sent to all new referees when an assessment is booked and they also have a further opportunity to read the notice in the centre when they sign up for the service.

4.8. The client may decline/withdraw consent to receive Acacia marketing and promotion without detriment to the support service they are receiving.

4.9 The National Opt Out policy gives all clients the right to opt out of using their confidential information for planning and research. This is contained in the privacy notice. If a client wishes to opt out they should be referred to Rob Ewers the Data Protection Manager to progress.

5 Disclosing Information: ***when a decision is made regarding the sharing of information it should be guided by the 7 golden rules of sharing.***



5.1. In normal circumstances, staff may only disclose personal information outside the organisation if one or more of the following applies:

5.1.1. The disclosure is routinely necessary for the purpose for which the information is held and the individuals about whom the data is held have been made aware of, or could reasonably expect, such a disclosure to be made as part of the legitimate interests of the service.

5.1.3. The receiving staff member 'needs to know' the information in order to carry out their duties;

5.1.4. The person about whom the information is held has given valid consent to the disclosure

5.2. Where it is not possible to obtain valid consent, information may exceptionally be passed on when there is a legal basis for overriding the usual non-disclosure e.g.

5.2.1. The disclosure is required under direction of a Court Order'

5.2.2. The disclosure is provided for agreed inter-agency procedures which have a legal basis for their operation.

5.2.2. Imminent safety risk for client or other, including safeguarding concerns. In these situations consult with designated safeguarding lead if advice needed. Only share the information which is necessary and appropriate to address safeguarding needs.

5.3. When passing information to others, staff should:

5.3.1. Check that the source of the request is bona fide;

5.3.2. Ensure that the recipients understand and accept their obligation to respect the confidentiality of the information;

5.3.3. Only send the information necessary for the purpose of the disclosure;

5.3.4. Record exactly what has been passed on, to whom, when and why in the Acacia database or other appropriate place.

5.3.4. Ensure that FQ038a Limitations of Use Statement is included in any written/printed/faxed communication.

5.4. When receiving information from others, staff should:

5.4.1. Ensure that any information received in confidence should be marked as such to ensure it is not inadvertently disclosed to third parties;

5.4.2. Ensure that only information necessary for the purpose of the information being shared should be requested.

5.4.3. Ensure that information requests include a confidentiality statement similar to "Information will be treated with utmost confidence and will not be divulged to anyone outside the organisation except when stated at collection or agreed at a later date."

5.4.4. Add to database and shred paper communications where practicable.

5.5. All confidential information shall be treated in line with Acacia's Confidentiality & Data Protection Policy.

5.6 All staff employment job descriptions and volunteer role descriptions must contain a statement enforcing the duty to respect the confidentiality of information.

5.7. Staff, students, staff of other agencies, temporary staff and volunteers must sign a confidentiality statement (FQ008 Confidentiality and Data Protection Statement for volunteers or FQ008c Confidentiality Agreement Employee and Contractor) on commencing employment/placement with Acacia either as part of their staff contract or as a separate signed statement.

5.8. All employees and volunteers are responsible for:

5.8.1. Checking that any personal data that they provide to Acacia is accurate and up to date.

5.8.2. Informing Acacia of any changes to information which they have provided, e.g. changes of address.

5.9. Sensitive information is only to be requested on a 'need to know' basis. This means only when the information is necessary to provide a service or to manage the delivery of a service effectively.

5.10. The national data opt-out gives everyone the ability to stop health and social care organisations from sharing their confidential information for research and planning purposes, with some exceptions such as where there is a legal mandate/direction or an overriding public interest for example to help manage the covid-19 pandemic. Acacia will ensure that clients are made aware that they have the right to withhold consent for this category of data. This is stated clearly on our privacy notice.

6. Culture and Training

6.1. Acacia will ensure that staff, volunteers and trustees receive adequate training and guidance on their duties and responsibilities in relation to the handling, disclosure and storage of personal information and information assets and will be deemed suitable for the roles they are considered for to reduce the risk of theft, fraud or misuse.

6.1.1 A training needs analysis will be carried out/reviewed and implemented at least once per year.

6.1.2 All staff and volunteers will receive data protection training at an appropriate level for their role as part of their induction, with refreshers at least annually.

6.1.3 Training will include an assessment and at least 95% of all staff must successfully complete the training/assessment each year.

6.1.4 An enhanced level of training will be required for those with direct responsibility for data protection within the organisation.

6.2. All staff and volunteers must make every effort to participate in and complete Acacia Data Protection training in a timely manner.

6.3. Acacia will develop a culture of 'Privacy by design' by requiring data protection impact assessments (DPIA's) to be completed for any new project or change/addition to our IT structure and/or plans, and maintaining a raised profile of data protection through notices, reminders and inclusion of data protection at staff meetings.

6.4. In accordance with the organisation's disciplinary procedures, disciplinary action may be taken against any member of staff who fails to carry out the duties and responsibilities set out in this Policy or the procedures that follow from it.

6.5. Where contractors and employment agencies are used, the contracts between Acacia and these third parties will contain clauses to ensure that contracted staff are bound by the same code of confidentiality and data protection as employed staff.

6.6. Procedures must be maintained and implemented to ensure an employee's, contractors or third party's exit from Acacia is managed and the return of all equipment and removal of all access rights are completed.

6.7. Any breach of this policy will be taken seriously and may result in formal action. Any employee who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with Acacia's data protection manager Rob Ewers, Operations Director.

7. Acacia's Designated Data Controller/Data Protection Manager

7.1. Acacia is responsible for ensuring compliance with data protection legislation and implementation of this policy on behalf of the Trustees. Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with the Data Protection Manager. The Data Protection Manager Rob Ewers is the named individual responsible for operational data protection compliance within Acacia.

8. Data Security

8.1. The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. All staff are responsible for ensuring that:

8.1.1. Any personal data to which they have access is kept securely, either electronically or in lockable cabinets

8.1.2. Personal information is not disclosed either orally, in writing or otherwise to any unauthorised third party.

8.1.3. Written personal information taken off site must only be in essential circumstances.

8.1.4. Written records taken off site must be pseudo anonymised - they must never contain the client's name anywhere on the document or any other obvious identifying details.

8.1.5 The client's unique generated code must be used as an identifier in this information. The staff member must ensure the written information is kept securely offsite at all times.

8.1.6. Documents containing individual data must not be left visible where they can be read by anyone inappropriately. This includes telephone messages, computer prints, letters and other documents.

8.1.7. Desks must be cleared of any personal information each evening and electronic documents closed down when leaving a desk.

8.2. Users must be aware of their responsibilities for maintaining effective access controls, particularly regarding the use of computers, mobile devices and passwords. Protection will be required commensurate with the risks when using mobile computing and remote working facilities as per PQ18a Computer and Mobile Device Policy. This policy must be read in conjunction with PQ18a, which give further details of the security measures which Acacia maintains and which must be adhered to by all staff and volunteers.

8.3. All hardware containing data must be handled securely being mindful of the above protocols and policy.

8.4. Personal data must not be stored on the hard disc of an Acacia laptop or flash drive unless it has been encrypted and secured by robust password as per policy guidelines.

8.5. Access to system files and program source code will be controlled and information technology projects and support activities conducted in a secure manner including sufficient firewall.

8.6. All equipment containing storage media will be checked to ensure that any sensitive data and licensed software has been removed prior to passing on to Orbits for secure disposal. During this process all remaining data is securely overwritten prior to destruction and Orbits will provide Acacia with a certificate of secure disposal.

8.7. Acacia will ensure and verify that all personal data held by us and our data processors will be stored in a secure manner. Ensuring physical and environmental security is in place to prevent unauthorised physical access, damage, theft, compromise, and interference with personal information. Robust cyber security measures must also be in place.

8.7.1. Acacia shall ensure that personal data is stored securely using current security software that is kept-up-to-date by OrbitsIT.
8.7.2. In order to provide enhanced security Acacia will maintain M365 Business Premium licensing incorporating Windows Defender for Business, Azure and InTune
8.7.3. Appropriate back-up and disaster recovery solutions shall be in place.
8.7.4. All cloud based personal data shall be stored securely inside the EU. Acacia requires all cloud-based providers to use industry standard security/backup and provide details of this to Acacia for our records. If data is stored/processed outside the EU it must be done so under the same robust security and confidentiality conditions as those required inside the EU.

8.8. All health records including client's personal and special category information data will be stored on the Acacia electronic client management system which is hosted in the EU. This service is currently provided by iizuka. A GDPR/data protection legislation compliant contract must be maintained with these

processors to ensure security of data. Client paper files will be secured at head office in locked filing cabinets.

8.9. As a small organisation, Acacia uses a cloud-based version of Microsoft Office 365. As a result, our data is stored in the Microsoft Cloud which is based in the EU. In the unlikely event that we transfer personal information to countries that are outside of the European Union we will ensure that the transfer is carried out in a compliant manner and appropriate safeguards are in place.

8.10. Document tracking – all hard copy client files must be stored securely at head office. In rare instances if there is a necessity for the file to be taken off site the permission of the Data Manager, Rob Ewers, must be obtained and the file must be tracked, kept secure at all times, and returned to head office as soon as possible.

8.11. Passwords for all system accounts, Infrastructure accounts (e.g. Wi-Fi), social media accounts and all computers and mobile devices must always be changed from default values and should have high strength. See mobile device policy for further information.

Please see Appendix One for security information relating to the use of iizuka the client database.

9. Subject Access Requests

9.2. In accordance with individuals' rights of access under the data protection legislation, Acacia will, on request, inform an individual what information is kept about them and will provide a copy of that information. Any person who wishes to exercise this right should make the request in writing to the Data Protection Manager using the standard form (FQ008m Subject Access Request). *Please note that the request does not have to be made using only this form and the individual has the right to make the request in writing in any format they wish. This form has been provided to assist the individual and Acacia by providing a simple and systematic template for the request.*

9.3. If personal details are inaccurate, they can be amended upon request
9.4. Acacia aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within 30 days of receipt of a completed form/request unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request.

9.5. All individuals who are the subject of personal data held by Acacia are entitled to:

9.5.1. Ask what information the organisation holds about them and why.
9.5.2. Ask how to gain access to it.
9.5.3. Be informed how to keep it up to date.

9.5.4. Be informed what the organisation is doing to comply with its obligations under the Data Protection legislation

9.5.4 . Be provided with a copy of it

9.5.5 Have that information deleted/destroyed – unless it is:

i. a health record, in which case Acacia is required to keep this information securely for 8 years to comply with Records Management Code of Practice for Health and Social Care, IGA, 2016.

ii. Or must be kept to comply with employment legislation or other relevant legislation/legal requirement

10. Outsourcing

10.1. It is inevitable that Acacia must outsource various IT services and facilities i.e. cloud based storage, cloud base database, IT support services. To ensure that these outside services or 'data processors' do not present any additional risks to the security of personal information Acacia clearly specifies how these services should manage personal data and restricts their processing of it by specifying this in our contracts.

10.1.1. Acacia requires data processors to have good security and internal privacy policies to be in place and adhered to.

10.1.2. These data processors are specifically identified in the Acacia Data Protection Map and Data Protection Register

10.1.2. The individual has a right to know who these outsourced services are and how they are involved in processing their information. This information is included in the privacy notice.

11. Collection and Retention of Data

11.1. The purpose for holding personal data and a general description of the categories of people and organisations to whom we may disclose it are listed in the Data Protection register and the Data Map . This information is available in the data protection folder on Sharepoint or may be obtained from the Data Protection Manager, Rob Ewers.

11.2. Acacia recognises The Records Management Code of Practice for Health and Social Care (IGA, 2016) as the basis of our health records management and retention procedures. Health records are to be kept for 8 years in line with this guidance.

11.3. Human resources information is kept for the duration of employment or volunteering with Acacia and in line with employment legislation for 6 years after in most cases but can be as much as 18 years for some.

11.4. Following the appropriate retention period all data, whether hard copy or computer data is permanently deleted. Hard copy notes are cross shredded to an extent that they are irretrievable. See 13 below.

12. Auditing of data protection

12.1. The various processes regarding data management and security are built into the standard audit cycle to ensure compliance with this policy.

12.2. Acacia will test data protection procedures eg. breach process to ensure that our practices and policies are effective and robust.

12.3. Staff should be aware that Acacia carries out spot checks to ensure that all staff are being compliant with confidentiality, data protection and mobile device policy. The spot checks are carried out at least annually and also include spot checking the use of own mobile devices.

13. Archiving / Removal

13.1. Our aim is to store personal information for the shortest time necessary to complete the purposes for which the information was gathered. This is a directive and a client right under GDPR legislation. To ensure that personal data is kept for no longer than necessary Acacia only keeps personal information according to the time periods recommended by applicable guidelines and legislative requirement. The specific time periods are stated in the relevant privacy notice.

13.2. Acacia will keep some forms of information for longer than others depending on a number of factors e.g. NHS contractual requirements, health record guidance, legal obligation. All staff are responsible for ensuring that personal information is not kept for longer than necessary

12.2. Disposal of information no longer required must maintain privacy and confidentiality. Paper copies must be shredded. Electronic records must be permanently deleted as per 8.6.

13. Breach

13.1. Acacia has an obligation to report personal data breaches to the Information Commissioner's Office within 72 hours of becoming aware of the breach. Information regarding data loss and or breach of security incidents must be communicated to the Data Protection Manager in a timely manner to allow the appropriate action to be taken. PQ018c Personal Data Breaches provides guidance for staff and volunteers where a breach is suspected/observed/discovered.

13.2. In the event of the discovery of an internal breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, this information must be reported to The Data Manager immediately. The Data Manager will act to promptly assess the risk to people's information, rights and freedoms and if appropriate report this breach to the ICO within 72 hours. The Data

Protection Manager will refer to PQ 018b Breach Incident Management Plan Template as a guide and record the breach and consequent action in the breach incident register.

13.3. In the event of the discovery of an external breach i.e. in one of our data processors, we will expect this to be reported to us immediately on discovery, bearing in mind that we will have to report the breach within 72 hours. This clause will be required in all contracting of external services who are data processors for Acacia.

14. Service Planning

14.1 When considering changes to any of our service provision the organisation will consider whether it needs to carry out a DPIA at the early stages of any new project if it plans to process personal data. A DPIA should follow relevant guidance from the Information Commissioner's Office (ICO). This process will be overseen and co-ordinated by the Data Protection Manger Rob Ewers.

Appendix One – Accessing the Database – Security Considerations

At the core of Acacia's service is our iizuka client database 'Case Manager' which is where we store all client data including their health record. This information is highly sensitive and personal and the impact of losing or breaching this data could be great and have serious consequences for the individual and the organisation. Therefore, it is vitally important that we pay particular attention to keeping this information safe and secure.

The following requirements are here to help ensure that we follow safe practices in relation to accessing the client database and minimise the risk of loss and/or breach.

- Only authorised staff and volunteers should access the client database and you must never access client personal data unless you have a specific need to do so in relation to the delivery of the service.

- The database is password protected with 2 factor authentication utilising Azure – all staff and volunteers accessing the database should use their own password. This must not be shared. The database has an internal auditing system which identifies each login and records all activity whilst you are logged in.

- Computers/Laptops which are used to access the database must be approved Acacia devices. They must be full protected/encrypted and must comply with the security requirements of PQ018a Computer and Mobile Device Policy.

- You must never download personal information from the database to your computer. The only exception to this is fully anonymised summative data for reporting purposes.

- Never leave your computer/mobile device unattended with the client database portal open.

- Never access the database where other persons may be able to view the information on your screen.

- Any device used to access the database must have a 5-minute time out set so that it goes into standby when no activity is detected and requires a password to log back in.

- Never store your password together with your computer/laptop. If passwords are stored they must be encrypted and/or kept in a secure location with no additional identifying information regarding what the password relates to.

- When a case holder who is a registered user of Case Manager takes extended leave of any kind (more than four weeks) it is normal practice for their iizuka access to be suspended whilst they are on leave. This is primarily to reduce unnecessary risk of unauthorized access/breach but has the additional advantage of helping the staff member to completely disengage from work, protecting them from the temptation to check how their client is doing and/or being tempted to work when on long term leave. Furthermore, if this specifically relates to anxiety/stress related leave, their access may be suspended sooner during their leave period, protecting them from potential triggering information. In all instances, the staff member should be informed and reminded why the temporary suspension of access is put in place. This will hopefully allay any confusion or concern by the staff member as to why this action has taken place.