Data Protection &
Information Sharing and Security Policy

Agreed by the Board: Jan 2013

Last Reviewed: Jan 2021[1]

Review Date: Jan 2022

Overview

Application of this policy will be on the basis of equal opportunities regardless of race, colour, nationality, or ethnic origins, age, marital status, gender, sexual orientation, disability, religion or other personal circumstances or disadvantages.

This Policy describes how Oasis Project meets its legal obligations and requirements concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the General Data Protection Regulation (GDPR) as interpreted in UK statute as the Data Protection Act 2018 and the common law Duty of Confidentiality.

[1] Amendments Jan 2020: Update title to Data Protection and Information Sharing and Security Policy to comply with cyber security recommendations. Email protocol further strengthened by way of password protection guidance.

1. Contents

1. Legislative Framework

General Data Protection Regulation
Data Protection Act 2018
Common Law Duty of Confidentiality
Children's Act 1989 & 2004
Computer Misuse Act 1990
Human Rights Act 1998
Crime and Disorder Act 1998
The Protection of Children Act 1999
Working Together to Safeguard Children 2015
Freedom of Information Act 2000
Health & Social Care Act 2012
Sexual Offences Act 2003
Privacy and Electronic Communications Regulation (2016)

2. National Guidance and Local Protocols

Confidentiality NHS Code of Practice (2003)
ICO Data Protection Self-Assessment Kit (2018)
Information sharing advice for safeguarding practitioners (2015)
Retention of Volunteer Personal Information (2015)
Record Management Code of Practice for health and Social Care: Information Governance alliance (2016)

3. Other Relevant Policies/ Procedures/ Guidelines

Confidentiality Policy
Safeguarding Children Policy
Staff Code of Conduct
Adult Safeguarding Policy
Right to be Forgotten Policy
Fraud Prevention Policy
Fraud Response Plan Flowchart
Incident Management Policy
Disciplinary Policy
Rights and Responsibilities Charter
ICO guide to data protection

4. Scope of Policy

- This policy applies to all Oasis management, employees, volunteers, and service users.
- This policy is applicable both on and off premises during Oasis related activities.
- Oasis recognises service users, volunteers, staff, partner agencies and donors as data subjects.

5. Core Terminology

Term	*Definition*
Data Subject	Any living person Oasis stores Personal or Special Category data on.
Personal Data	Any data that can identify a living person.
Special Category data	(Formerly 'Sensitive Data') Any data relating to Protected Characteristics under the Equalities Act, health, wellbeing, or criminal activity.
Data Controller	Any organisation that has decision-making control over which data is stored and used.
Data Processor	Any Organisation contracted to handle data on behalf of a Data Controller.
Data Protection Officer	The lead person tasked with ensuring compliance with DPA2018, giving full consideration to the Data Subjects.
Information Asset Owners	Any Manager who makes decisions around day to day use of data.
Senior Information Asset Owner	The CEO
Senior Information Risk Owner	A member of the Board of Trustees with overall corporate responsibility for GDPR compliance

6. Policy Statement

Oasis Project needs to collect and use data about people using or associated with the organisation in order to operate and carry out its functions effectively. These may include current, past, and prospective service users, employees, donors and volunteers (data subjects).

Organisations involved in providing services to the public have a legal responsibility to ensure that their use of personal information is lawful, properly controlled and that an individual's rights are respected. Oasis Project regards the lawful and appropriate treatment of all personal information as crucial to successful service delivery and essential to maintaining confidence between the organisation and those individuals who are involved with it. The organisation therefore fully endorses and adheres to the Principles of Data Protection under Article 5 of the GDPR.

Mindful of data security, Government policy allows agencies to work across boundaries to provide services on a multi-agency basis according to the needs of service users. Essential information must, therefore, be able to pass between the Substance Misuse Services, NHS, Local Authority, Social Services and other services (such as housing, youth offending team, education, voluntary or

independent bodies) where those organisations are contributing to, or planning, a programme of care, or where one may need to be initiated.

The balance between the need to share information to provide quality service and protection of confidentiality is often a difficult one to achieve.

This policy, in conjunction with the GDPR, our Safeguarding Children, Adult Safeguarding and Confidentiality Policies, aims to clarify and guide this balance.

Depending on the nature of the contract that Oasis Project has with a funder, Oasis Project will always have one of two statuses:

a. As a Data Controller, with overall responsibility for how a data subject's data is gathered, used and stored. In this case Oasis' policy, protocols and understanding of best practice under GDPR is applied.
b. Or, as a Data Processor, working in partnership with a funder to carry out a task on their behalf (e.g. Care coordination). In this case, we legally agree to follow the instructions of the funder who is the Data Controller. Where Oasis Project acts as a Data Processor, we will always ensure the Data Controller is tasking us clearly and within the safest application of GDPR.

7. Relevant Procedures & Implementation Guidelines

7.1 Training & Dissemination of Information

All employees will be made aware at induction of their responsibilities under the terms of this policy and the GDPR, including reasonable precautions necessary to securely record and share data.

All Staff will have full access to this Policy, any Protocols giving specific guidance and the Advice and Guidance of their management.

Modifications and updates to data protection and information sharing policies, legislation, or guidelines will be brought to the attention of all staff.

Service users will be informed of our duties under the Data Protection Act 2018 as part of their induction into services and a signed consent form to share information will be kept with their file.

7.2 Advice & Consultancy

Where reasonably practical all relevant staff will be consulted on modifications and updates to procedures relating to data protection and information sharing.

The following agencies could also be consulted on specific confidentiality and information sharing matters:

The Information Commissioner's Office

Commissioning/Funding bodies
Service User Advisory Groups
Third Party legal Advisors

7.3 Employee Contracts

Each employee will sign a confidentiality (non-disclosure) undertaking as part of their contract of employment and will be personally responsible for ensuring there are no breaches of confidentiality in relation to any personal data, however it is stored. Employees should also be mindful of their professional code of conduct or the codes of conduct from other professions that they are aligned to (such as Social Work or Nursing). Failure to comply will result in the instigation of a disciplinary procedure.

7.4 Article 5 of GDPR and corresponding duties

The Data Protection Act 2018 became law in May 2018 and covers personal information relating to living individuals that is held in any media e.g. paper files, computer records, audio and video tape, etc.
The Data protection Act 2018 is the enshrining in UK law of the EU's General Data Protection Regulation. Insofar as the rights of data subjects and the responsibilities of organisations are concerned, the Data Protection Act 2018 and GDPR can be equally referenced.

There are six key principles of data management outlined in Article 5 of the GDPR. These principles are defined below and Oasis' response to them is outlined.

Article 5 of the GDPR requires that personal data shall be:

a. "Processed lawfully, fairly and in a transparent manner in relation to individuals."

Oasis Project recognises that it can process personal data where one of the following conditions has been met:

- The data subject has consented to the processing
- Processing is necessary for the performance of a contract/agreement with the data subject
- Processing is required under a legal obligation, usually in the public interest.
- Processing is necessary to protect the vital interests of the data subject.

All data subjects are to be made aware who the data controller is, the purposes for which the data will be processed, the likely consequences of the processing and how data is shared.

All data subjects of Oasis Project must give their explicit consent for the gathering and processing of special category data unless the processing is required by law for employment purposes or for administration of justice or legal proceedings or to protect the vital interests of the data subject (e.g. in a child protection case).

Special Category Personal Data (formerly *Sensitive data*) includes their racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sexuality or criminal proceedings or convictions. Any non-routine disclosure of information must be approved by the CEO who is the Senior Information Asset Owner and the Caldicott Guardian. Non-routine disclosure requests for which there is no legislative requirement to share information (for example, reference requests for clients by commercial companies) will only be authorised by the Senior Information Asset Owner if the client has given explicit consent, in consultation with the Data Subject if appropriate, and only in circumstances where the Data Subject would not be adversely affected by so doing.

All data subjects have the right to refuse consent to process their data. If a subject withholds consent to process their personal data, this will be respected, but it may mean that Oasis is unable to work with the subject, and in the case of an employee or volunteer, they would be unable to take up a position with the organisation. GDPR asks that services should not be wholly conditional on consent to provide data (for example, if a client wishes to use a pseudonym and withhold their name, Oasis must take into consideration if it can still offer a service - there will be times that a service can be offered and times when it cannot).
Oasis will never seek to use data unlawfully and employs suitable checks and balances to prevent against this.

b. "Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;"

Through the use of explicitly worded and readily available privacy notices, Oasis ensures that all data subjects are clear that staff are collecting, storing and using personal data only for specified purposes.

There is an onus on all frontline staff to ensure that the specified purpose for which data is being gathered is clearly, and regularly, explained to data subjects. If a staff member is unclear themselves why they are collecting a piece of data, they must take professional responsibility for discussing this with their manager.

Data Protection by design is interpreted to mean that all project-planning includes full and thorough discussion and planning on how data will be collected, stored and used for what clearly specified purpose.

Information Asset Owners (Service Managers) should have a full understand of what data their teams are collecting, and for what specified purposes. They should have regular briefings with staff to make these specified purposes clear, so staff can then explain to data subjects.

Where Oasis is collecting data where the data is no longer useful for clearly specified purposes the Data Protection Office will advise the Information Asset Owners on best practice and this data will be

deleted.

Oasis will not pass personal information to any third party without clear consent from Data Subject, except where data may be vital for the protection of a person, or the prevention of a serious crime.

c. "Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;"

And,

d. "Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;"

In response, all Oasis client records should follow the following guidance:

- Always date and sign/initial records.
- Record information as soon after the contact as possible to maintain high levels of accuracy.
- Record in a style that is legible, able to be photocopied, and cannot be easily changed or deleted.
- Changes/modifications of records should be dated and signed.
- Do not include jargon or abbreviations.
- Do not include irrelevant information.
- Clearly differentiate between matters of fact and opinion.
- Do not express opinions that you are not prepared to defend, or which you cannot substantiate.
- Do not express opinions in areas where you are not qualified.
- Always be sure of the facts.
- Do not write in anger or in haste. This is particular danger with e-mails because of the immediacy of e-mail as a means of communication.
- Always speak respectfully of the person, even when expressing negative information.

e. "Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;…"

Oasis retains data for no longer than it is necessary. See Data Retention Periods (section 10) which follow best practice guidance within the Record Management Code of Practice for Health and Social Care 2016 (Information Governance Alliance)

We will keep any client, volunteer or employee records as advised by legal representatives, where legal action has been started.

f. "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."

All Records in Oasis Project are kept safely, with systems in place to minimise the risk of a breach.

All electronic records are kept in secure environments only accessible to Oasis and their contracted ICT providers.

All paper records are retained in locked buildings and in locked cabinets. Transportation of Personal Data is kept to a necessary minimum.

Oasis Project's Risk Management Policy includes an analysis of risk in relation to electronic and manual information records.

Any security breaches will be logged, investigated and monitored via the Quality Assurance and Risk Management Sub Group of the Board of Trustees.

7.5 Passwords

Passwords are a key part of the IT strategy to make sure only authorised people can access relevant resources and data. All staff who have access to any of those resources are responsible for choosing strong passwords and protecting their log-in information from unauthorised access.

The purpose of this policy is to make sure all Oasis resources and data receive adequate password protection.

7.6 Password creation

- All passwords should be reasonably complex and difficult for unauthorised people to guess and they should not contain reference to any personal identifiable information, e.g. road names, children's names, pet names. Staff should choose passwords that are at least 14 characters long and contain a combination of upper- and lower-case letters, numbers, and punctuation marks and other special characters.
- In addition to meeting those requirements, staff must avoid basic combinations that are easy to crack. For instance, choices like "password," "password1" and "Pa$$w0rd" are not acceptable.

- A password should be unique, with meaning only to the person who chooses it. That means names, places, common phrases should be avoided.
    - A recommended method for choosing a strong password that is still easy to remember is to pick a phrase; take its initials and replace some of those letters with numbers and other characters and mix up the capitalisation.
    - Or pick a random word that has no personal meaning to you and add a number.
- All passwords must ideally be changed regularly, with the frequency varying based on the sensitivity of the account in question.
- If the security of a password is in doubt– for example, if it appears that an unauthorised person has logged in to the account — the password must be changed immediately.

7.6 Protecting passwords

- Staff must never share their passwords with anyone else within the organisation including co-workers, managers, administrative assistants, IT staff members, etc. Everyone who needs access to a system will be given their own unique password.
- Staff must never share their passwords with any outside parties.
- Staff should take steps to avoid phishing scams and other attempts by hackers to steal passwords and other sensitive information.
- Staff must refrain from writing passwords down and keeping them at their workstations. See above for advice on creating memorable but secure passwords.

8. Addressing concerns and actions on behalf of Data Subjects

1.1 Right of Access

This is also known as a Subject Access Request (SAR). The DPA 2018 is clear that:

> Data Protection Act 2018
>
> 94 Right of access
>
> (1) An individual is entitled to obtain from a controller— (a) confirmation as to whether or not personal data concerning the individual is being processed, and (b) where that is the case— (i) communication, in intelligible form, of the personal data of which that individual is the data subject, and (ii) the information set out in subsection (2).
>
> (2) That information is— (a) the purposes of and legal basis for the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipients to whom the personal data has been disclosed; (d) the period for which the personal data is to be preserved; (e) the existence of a data subject's rights to rectification and erasure of personal data (see section 100); (f) the right to lodge a complaint with the

Commissioner and the contact details of the Commissioner; (g) any information about the origin of the personal data concerned.

In response, should a Data Subject request access to the data held about them, Oasis Project will always work to meet that request in a way that is clear, within due time limits and mindful of best practice in safeguarding.

Where Oasis Project is a Data Controller, staff will be asked to follow the **Subject Access Request Protocol**.

The Data Protection Act 2018 is explicit that: '(6) Where a controller cannot comply with the request without disclosing information relating to another individual who can be identified from that information, the controller is not obliged to comply with the request…'

The Subject Access Request Protocol gives instruction to the Data Protection Officer on when and how data should be redacted or a Subject Access Request should be refused.

1.2 Data Breaches

A Data Breach has occurred when a person or persons not employed by Oasis Project gains access to the Personal or Special Category data of any data subject whose data we have legally consented to retain safely.

Recital 85 of GDPR "A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

Application of best practice within Oasis, and consideration of *Data Protection by Design* will limit the risk of a Data Breach. Risk Management is carried out through the Quality Assurance and Risk Management Sub Group of the Board of Trustees. All potential areas of risk are mapped for their likelihood and impact should they occur.

If a data breach is to occur, there is a duty on Oasis to act quickly and effectively to:

- Minimise the risks.
- Communicate with affected Data Subjects.
- Communicate with the ICO.

- Investigate the incident fully: an incident form will also need to be completed. If a member of staff is found to be in breach, they may be subject to disciplinary proceedings in line with the Disciplinary Policy.
- Follow any recommendations of investigation or investigation by the ICO.
- If a mobile device has been lost, contact the service provider to ensure that the device is disabled immediately.
- Inform the CJSM helpdesk if any such data is breached when using CJSM email.

All investigations into a Data Breach must be coordinated by the Data Protection Officer who must been seen by the Data Subject and ICO to independently analyse root causes of any breach with regards of the rights of the Data Subject over the requirements of the Organisation.

The Data Protection Officer should be guided by the Data Breach Protocol when responding to a Data Breach.

If data has been lost, or misplaced, but not knowingly accessed by any person (e.g. a laptop left on public transport), this should be considered a *near miss.* The Data Protection Officer will organise a suitable response but under the DPA 2018 is not obliged to inform the data subject or the ICO if the potential risk to the data subject was minimal.

1.3 Right to be forgotten

This is also known as the 'Right of Erasure'

A17 of GDPR

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

1. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

2. the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

3. the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

Where Oasis Project is the Data Processor such a request will be passed to the Data Controllers.

Where Oasis Project is the Data Controller all requests will be respected but responded to mindful of the charity's legitimate interests in providing services to clients who may be vulnerable and the consequent public interest in ensuring safeguarding and preventing offending.

The Data Protection Officer is the lead for managing all Rights to be Forgotten. **The Right to be Forgotten Protocol** will guide the DPO in this matter.

1.4 Data Retention periods

Oasis Project Retains Data Subjects' data for these periods:

Type of Record – Service Users	**Duration of Retention**
Adult service user files (inactive)	5 years after conclusion of treatment
Children and Young People's records (under 18)	5 years after conclusion of treatment
Type of Record – Employees / Applicants	**Duration of Retention**
Unsuccessful recruitment candidates not shortlisted	60 days from closing date of recruitment.
Unsuccessful recruitment candidates shortlisted but not selected	60 days from closing date of recruitment
References received	6 years
Annual Leave records	6 years
Sickness records	6 years
Unpaid / Special Leave records	6 years
Annual Appraisal / Assessment Records	6 years
Payroll and Tax Information	6 years
Records relating to accident or injury at work	3 year from end of employment
Application form	Duration of employment
Records relating to promotion, training, disciplinary matters	6 years from reference / end of employment
References given / information to enable reference to be provided	6 years from reference / end of employment

Summary of record of service (eg name, position(s) held, dates of employment)	10 years from end of employment
Type of Record – Volunteers	**Duration of Retention**
Unsuccessful volunteer applicants	60 days from closing date of recruitment
Volunteer application form	Duration of volunteering
Other volunteer records	1 year

Note, at the end of the five year period relating to Service User records, Oasis will, with clear explanation, have the legal right to decide to retain records for longer period. The Data Protection Officer will lead on this decision. This will only happen where there have been known safeguarding or offending risks and it is reasonably believed Oasis may have to present evidence at some future legal forum.

9. Consent to Share Information Relating to Service Users

All data held on service users is obtained and stored for an explicit purpose which is made clearly known to the service user. It is common for Oasis to share data with other agencies involved in the support of service users. There is a reasonable legal basis to share with other support providers when the service user has provided consent that is:

- **Unambiguous**
    - Consent to share information with one agency does not automatically guarantee consent to share with another.
    - Consent to share particular information with an agency, does automatically guarantee that all information can be shared.

- **Active**
    - Oasis must know and record that a service user using a service for a longer duration still consents to information sharing.
- **Revokable**
    - Consent can be revoked at any time.

Oasis must take every reasonable action to ensure that service users are clear on their rights and that they clearly consent to information-sharing.

Any worker disclosing information to a third party without the service user's permission, except in exceptional circumstances (see below) will be subject to disciplinary procedures.

10. The Caldicott Guardian

A Caldicott Guardian is a senior person responsible for protecting the confidentiality of service user information and enabling appropriate information-sharing. The Guardian plays a key role in ensuring

that the NHS, Councils with Social Services responsibilities (CSSRs) and partner organisations satisfy the highest practicable standards for handling patient identifiable information.

Within Oasis the Caldicott Guardian is the CEO. The key responsibilities of the Caldicott Guardian are as follows:

Strategy & Governance: the Caldicott Guardian should champion confidentiality issues at Board/management team level, should sit on an organisation's Information Governance Board/Group and act as both the 'conscience' of the organisation and as an enabler for appropriate information sharing.

Confidentiality & Data Protection expertise: the Caldicott Guardian should develop a knowledge of confidentiality and data protection matters, drawing upon support staff working within an organisation's Caldicott function but also on external sources of advice and guidance where available.

Internal Information Processing: the Caldicott Guardian should ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff. The key areas of work that need to be addressed by the organisation's Caldicott function are detailed in the Information Governance Toolkit.

Information Sharing: the Caldicott Guardian should oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS and CSSRs. This includes flows of information to and from partner agencies, sharing through the NHS Care Records Service (NHS CRS) and related IT systems, disclosure to research interests and disclosure to the police.

It is the key role of the Caldicott Guardian to decide when the rights of the data subject to Privacy must be waived in favour of ensuring safeguarding in the public interest.

Oasis Project should display posters and/or leaflets explaining:

1. Who the Data Controller is (e.g. the organisation who owns the data)
2. Why the information is needed
3. The purposes for which the information will be processed
4. Who will see the information (secretaries, administration staff)
5. The benefits to service users and to the organisation(s)
6. Any disclosures that may need to be made to other organisations (e.g. Acute Hospitals, Social Services, Meals on Wheels, Clinical Audit, GP Payments, Mental Health Teams, Drug Teams etc.)
7. The circumstances in which information may be passed on without consent (e.g., Child Protection, and Crime and Disorder)
8. Information restricted by legislation (e.g. HIV, Termination, etc.)
9. Information that must be passed on because of legislation (Births, Deaths, Cancer Registries etc.)

These posters and/or leaflets should be made available in other languages for those whose first language is not English or in a different form for those with a disability.

11. Disclosure of Information without Consent

Any child protection, criminal or substantial concerns about risk to a person's safety, can override any confidentiality agreement.

Decisions to disclose information about a service user to a third party without the service user's consent ideally should be discussed by at least that individual's key worker and the Services Care Co-Ordinator/ CEO (the designated Caldicott Guardian), after an attempt has been made to persuade the service user to give consent. The final decision will be the Services Care Co-ordinator's/ CEO's, or in their absence, the most senior worker's. The decision should be made without delay ensuring compliance with any local agreements for safeguarding vulnerable adults and children. The client will be informed of the Project's decision wherever possible.

In certain other circumstances, information may be shared without the permission of the individual concerned:

- Where there are concerns about the welfare of a child as defined by the Children Act 1989 (see Child Protection Policy)
- When required through a court order, or through a legitimate search warrant
- If a violent situation arises and the service user is endangering the safety of staff, other clients, or others
- Where there are suspicions that a serious crime has or may be committed, e.g. murder, sexual crime (as defined in the Sexual Offences Act 2003), terrorism (as defined in the Terrorism Act 2000), drug trafficking (as defined in the Drug Trafficking Act 1994)
    - Section 115 of the Crime and Disorder Act 1998 gives public bodies the power, *but not a duty,* to disclose information for the prevention or detection of crime
- When disclosures of physical or sexual abuse are made and others may still be at risk from the alleged perpetrator
- When allegations are made of a gross breach of trust or misconduct of a professional worker
- Circumstances where withholding information might result in serious harm to another

- To ensure the service provides a duty of care in a life-threatening situation (e.g. serious illness or injury, suicide and self-harming behaviour). This includes when a service user continues to drive against medical advice, when unfit to do so. In such circumstances relevant information should be disclosed to the medical advisor of the Driver and Vehicle Licensing Agency (DVLA) as soon as possible.

The responsibility for the final decision for divulging information to a third party without the client's permission lies with the CEO (the Caldicott Guardian) or in her absence, the most senior worker.

12. Accessing Information without Consent

Employees may have the ability to access confidential information regarding individuals who are not service users, or information about service users that is not relevant to their work. It is an offence to access secure information without consent under The Computer Misuse Act 1990. Disciplinary action will be taken against staff members who have misused their privilege to access confidential information.

12.1 Unacceptable use of the internet

Unacceptable use of the Internet by employees includes, but is not limited to:

- Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via Oasis' email service
- Using computers to perpetrate any form of fraud, and/or software, film or music piracy
- Stealing, using, or disclosing someone else's password without authorisation
- Downloading, copying or pirating software and electronic files that are copyrighted or without authorisation
- Hacking into unauthorised websites
- Sending or posting information that is defamatory to the company, its products/services, colleagues and/or customers
- Introducing malicious software onto the company network and/or jeopardising the security of the organization's electronic communications systems
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities
- Passing off personal views as representing those of the organization

If an employee is unsure about what constituted acceptable Internet usage, then he/she should ask his/her supervisor for further guidance and clarification

All terms and conditions as stated in this document are applicable to all users of Oasis' network and Internet connection. All terms and conditions as stated in this document reflect an agreement of all parties and should be governed and interpreted in accordance with the policies and procedures mentioned above. Any user violating these policies is subject to disciplinary actions deemed appropriate by Oasis.

13. Information Sharing Security and emailing

No subject data will be given over the telephone unless the identity of the caller is verified. If the caller is unknown to the organisation, we will take a name and number and verify the caller's identity before disclosing service user information. Employees are required not to use identifiable information in emails, unless these can be encrypted.

The fax machine, answerphone and telephones are sited or used in an area that is restricted to those who need to access the information.

If a fax contains confidential information, ensure someone is at the receiving end waiting for it.

Where possible do not use identifiable information in faxes – use a client number. NB – where there is a risk of harm to children or adults, this does not apply, as full information including names should be communicated as soon as is practicably possible in any risk scenario, for example, a child protection referral or a notification of a violent incident.

Conversations which include confidential information should only take place within safe havens – i.e. behind closed doors.

13.1 Use of removable media

Use of removable media is restricted to Oasis usb sticks only. Staff are not permitted to use their own personal removable data. When the removable media needs destroying this needs to be done securely and evidence of this should be obtained. No-one other than staff will insert removable media into any Oasis equipment.

14. Recorded Data Security

All identifiable information held on service users must be kept secure – either in written/printed format in locked cabinets on premises, or in electronic format protected by passwords on an Oasis computer or on the Oasis virtual private network (VPN).

14.1 Written Records

Written records in which there is a client's name or enough information for a client to be identifiable to another party, should be kept in locked cabinets in areas where clients and the public do not have access at all times in which it is not in use. This includes at all times when the buildings are closed.

When not secured in cabinets, service user files or documents written about/by clients should not be left unattended in areas where non-staff members may be able to access them.

Files and records that contain person-identifiable information are disposed of either by shredding on site, or in the confidential waste bags which are subsequently sent to be shredded.

Service user files must not be removed from the premises.

14.2 Electronic Records

All electronically held confidential information must be protected by passwords, either on the VPN or on password protected computers provided by the organisation. These computers are equipped with the appropriate software to keep them as secure as is reasonably practicable (e.g. spyware scanners and firewalls) and the VPN password is regularly changed.

If computer hardware has ever been used to process personal data, it should only be disposed after reliable precautions have been taken to destroy any data stored.

All client information held on computer should be backed up every six weeks and back-up discs kept in lockable cabinets in areas where clients and the public do not have access unless accompanied by a staff member.

Any external contractors working on the Project's IT system or hardware, or working in the building, e.g. cleaners, must sign a confidentiality undertaking.

15. Information Sharing with the Police

Oasis recognises the need for effective liaison with the police service in the interests of the safety of service users, staff and visitors. Any contact with the police in relation to service users should be recorded on their file.

There may be situations where there is contact with the police which can be sensitive or difficult and staff should be reminded to seek advice if required, or if in doubt, as to how best to proceed. Advice should be sought from either your line manager or the CEO.

Service user records may be made available to the Police under section 29 and 35 Part IV of the Data Protection Act 1998, to assist in the detection of crime or the apprehension or prosecution of offenders. However, in accordance with the Caldicott Committee Report (1997), the provision of such information should be assessed as "the need to know".

In all circumstances, no information from any records should be released until a Section 29 Disclosure request has been signed by a senior police officer, detailing what information is required and why, has been provided by the requesting police officer. A receipt should also be obtained, which is signed by the officer taking the information, which records their name, rank, force number and base. Under normal circumstances original documentation will not be released, photocopies only will be provided.

Oasis Project is signed up to a third party reporting protocol which places a duty on staff to report to the police incidents that they have knowledge of in which a person has come to harm. For more information on this see the Third Party Reporting Protocol.

16. Responsibilities

The Board of Trustees

- Has overall responsibility for the policies and procedures at Oasis, so far as is reasonably practical.

The CEO

- To ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff.
- To Act as the Senior Information Asset Owner, making executive decisions on how to store and use data.

- Take the role of Caldicott Guardian and have ultimate responsibility for information sharing decisions where there is a safeguarding risk.
- To ensure that adequate resources and training is made available to staff on the subject of confidentiality.

Line Managers/Care Co-ordinators

- To act as Information Asset Owners, fully sighted on what information is stored in their service area and how it is stored.
- To ensure that staff members are adequately informed about data protection and confidentiality procedures at induction and that this is maintained within the working culture at Oasis

Staff Members & Volunteers

- To act with due care and attention for the Data Safety.
- To discuss any queries or concerns they may have about disclosures with a line manager or senior staff member.
- To ensure that the information they record or access is appropriately stored in secure cabinets or securely on computers.
- To ensure that they verify the authorisation of another person to ensure information is only passed on to those who have the right to see/hear it.
- Not to discuss confidential matters outside of work.
- To dispose of any confidential information in a secure manner (i.e. confidential shredding service, or emptied computer recycle bin).
- Not to access any confidential records/databases/files for personal reasons.
- To attend appropriate training as required.
- Allow computer software updates
- Report any instances where they may have clicked on a malicious/suspicious website.
- Report loss of any mobile data immediately to the Admin/Business Manager so that the device can be disabled.

17 References

Information sharing advice for safeguarding practitioners (2015), Department for Education
www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice

Information Sharing: Guidance for Practitioners and Managers (2008) -
http://webarchive.nationalarchives.gov.uk/20130401151715/https://www.education.gov.uk/publications/standard/publicationdetail/page1/DCSF-00807-2008

Confidentiality: NHS Code of Practice (2003) - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf

NHS – Access to Records (2003) - http://webarchive.nationalarchives.gov.uk/20130107105354/http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_112916

NHS – Caldicott Guardians https://www.igt.hscic.gov.uk/WhatsNewDocuments/The%20Role%20of%20the%20Caldicott%20Guardian%20-%20Workbook%20-%2028-03-2017-Published.docx

FDAP Code of Practice (2008) - http://www.fdap.org.uk/code_of_practice.php

Children's Act 1989 – http://www.legislation.gov.uk/ukpga/1989/41/contents

Children's Act 2014
http://www.legislation.gov.uk/ukpga/2014/6/contents/enacted

Computer Misuse Act 1990 - http://www.opsi.gov.uk/acts/acts1990/UKpga_19900018_en_1.htm

Drug Trafficking Act 1994 - http://www.opsi.gov.uk/ACTS/acts1994/ukpga_19940037_en_1

ICO information on GDPR and the Data Protection Act 2018
https://ico.org.uk/for-organisations/data-protection-act-2018/

Human Rights Act 1998 – http://www.opsi.gov.uk/ACTS/acts1998/ukpga_19980042_en_1

Crime and Disorder Act 1998 – http://www.opsi.gov.uk/acts/acts1998/ukpga_19980037_en_1

The Protection of Children Act 1999 – http://www.opsi.gov.uk/ACTS/acts1999/ukpga_19990014_en_1

Freedom of Information Act 2000 - http://www.opsi.gov.uk/Acts/acts2000/ukpga_20000036_en_1

Health & Social Care Act 2001 –

http://www.opsi.gov.uk/Acts/acts2001/ukpga_20010015_en_1

Sexual Offences Act 2003 – http://www.opsi.gov.uk/acts/acts2003/ukpga_20030042_en_1