3.3 – EDAS Data Protection Policy – October 2018

ESSENTIAL DRUG & ALCOHOL SERVICES

DATA PROTECTION ACT 2018 (DPA 2018) POLICY

Date of Adoption: October 2018 – Board Meeting 4 Signed: Lynda Clarke (EDAS Chair)
Date of next review: Board Meeting 4 - 2021 By Whom: EDAS Board of Trustees

This policy is to be read in conjunction with the following EDAS policies & procedures:
1.4 Information Technology Policy
2.3 Code of Conduct Guidelines
2.4 Workforce Development Policy

1. Introduction

This policy aims to provide Information regarding the Principles and Guidelines for implementation, use and practice of Data Protection at EDAS.

EDAS is committed to meeting its obligations under the Data Protection Act 2018 (DPA 2018) and will only use data appropriate to carry out the activities required to support our service users including case recording and to undertake our obligations to learners, employees and volunteers including personnel files.

EDAS acknowledges its responsibilities in the collection, storage and destruction of data in a timely and secure manner.

Our commissioners often require EDAS to collect and produce specific data for monitoring purposes including information on both staffing and service user outputs/outcomes. To this end, EDAS will ensure that those collecting, storing and deleting such information are aware of what they can and cannot collect and report.

EDAS endeavours to ensure that all staff understand their duties under the DPA.

2. The DPA applies to manually held as well as computerised data and covers health and other records.

The eight principles of the Act are that data shall be:

- Processed fairly and lawfully
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate

- Not kept for longer than is necessary
- Processed in line with the data subject's rights
- Secure
- Not transferred to countries outside the European Economic Area (EEA) without adequate protection.

Definitions

- Personal Data is divided into two definitions; **Personal Data** and **Sensitive Personal Data**.

- **Personal Data** is information that relates to a living identifiable individual. Examples may include:
- name
- address
- telephone number
- e-mail address

- **Sensitive Personal Data** is racial or ethnic origin, political opinions etc. Examples may include:

- Racial or ethnic origin
- Political opinions
- Religious or other beliefs
- Trade union membership
- Health
- Sexual orientation
- Criminal proceedings or convictions.

- It can only be processed:
- With explicit consent of the data subject (as per our confidentiality agreement)
- If required by law for employment purposes
- To protect vital interests of the data subject
- For administration of justice or legal proceedings.

- **Mobile Computing Equipment** includes:

- Portable computer devices - includes laptops, notebooks, tablet computers and Smartphones
- Removable data storage media - includes any physical item that can be used to store and/or move information and requires another device to access it. For example, CD, DVD, digital storage device (flash memory cards, USB memory sticks, portable hard drives). Essentially anything that data can be copied, saved or written to which can then be taken away and restored on another computer.

3. Responsibilities

EDAS will:

- ensure that there is a nominated individual with overall responsibility for data protection. Currently this person is the Chief Executive Officer (CEO)
- provide training for all staff members who handle personal information
- provide clear lines of reporting and supervision for compliance with data protection
- carry out regular checks to monitor and assess new systems for processing of personal data and to ensure that EDAS's notification to the Information Commissioner is updated to take account of any changes in processing of personal data
- develop and maintain DPA procedures.

All staff (including those working in or on behalf of EDAS such as volunteers, contractors, temporary staff, trustees, secondees and all permanent employees) will, through appropriate training and responsible management:

- Observe all forms of policy, procedures, guidance and codes of practice about the collection and use of personal information.
- Understand fully the purposes for which the EDAS uses personal information.
- Collect and process appropriate information, and only in accordance with the purposes for which it is to be used by EDAS to meet its service needs or legal requirements.
- Ensure the information is correctly inputted into specified reporting systems.
- Ensure the information is destroyed (in accordance with the provisions of the Act) when it is no longer required.
- On receipt of a request from an individual for information held about them by or on behalf of immediately notify their line manager.
- Not send any personal information outside of the United Kingdom without the authority of the Caldicott Guardian (Currently this person is the Chief Executive Officer (CEO)
- Ensure staff understand that breaches of this Policy may result in disciplinary action, including dismissal.

4. **Procedure**

Anyone handling information must comply with the GDPR Fair Processing Code. The Fair Processing Code says that Data controllers must continue to provide transparent information to data subjects. and that data subject must not have been misled or deceived as to the reasons why data was requested.. Under the act, data subjects have certain rights which include:

- To know if data is held about them on a computer system and be able to get a copy and description of that data
- To know the purpose(s) for which the data is being processed and who is going to receive the data
- To inspect such data and to have it changed if it is incorrect
- To ask for compensation if the data held is inaccurate or if unauthorised people have been given access to it
- To prevent the processing of data that is likely to cause damage or distress
- To make sure that decisions made against them are not made only on the basis of automatic processing

5. **When obtaining data from a data subject the following information must be readily available:**

- The organisation collecting the data is EDAS
- The identity of any nominated representative for the purposes of the Act (employee/volunteer)
- The purpose(s) for which the data will be processed
- Any other information necessary to ensure fairness, such as the likely consequences of the processing, and whether they envisage the data being disclosed to a third party.

6. Processing can only be carried out where one of the following conditions have been met:

- The data subject has consented to the processing.
- Processing is necessary for the performance of a contract with the data subject.
- Processing is required under a legal obligation.
- Processing is necessary to protect the vital interests of the data subject. Processing is necessary to carry out public functions.

When delivering services, the requirements of 4.2 and 4.3 are often covered at assessment as part of a discussion regarding confidentiality and consent and is recorded on the Pan Dorset Privacy Notice and NDTMS consent form.

7. Information can be shared with other professional agencies and significant others (e.g. families/carers) with the consent of the service user. Most information EDAS would want to share about a service user will be sensitive personal information (e.g. health), so explicit consent will need to be obtained. Personal information can be shared with other professional

- agencies without the service user's consent when there are child protection concerns or risk of harm to self, public or staff.

- For further information and support, staff should speak to their manager. Good practice is also detailed in the government publication Information Sharing: Guidance for Practitioners and Managers. Additional guidance is also available at Information sharing: further guidance on legal issues

8. **Staff must ensure that personal data is kept up-to-date and any mistakes corrected**

9. Personal data must only be held up to the point when the purpose for keeping the data has ceased. EDAS retains data for specified amounts of time in line with regulatory requirements and best practice guidance (only in exceptional circumstances should data be kept indefinitely). Staff must check with their manager if in doubt about the retention or destruction of data. (See **Appendix 1**).

10. Hard and soft data must be destroyed in a secure manner. EDAS has facilities for cross shredding paper at sites and there is a contract for secure disposal of paper at the EDAS Head Office. The individual is responsible for deleting any files from their system in accordance with **Appendix 1**. The IT consultants (Currently Target IT) alongside the Finance Manager are responsible for ensuring all data is removed properly from redundant computers (or transferred and stored appropriately) and checking data has been wiped from mobile computing equipment prior to approved re- allocation to staff.

11. **Personal data should be processed in accordance with the rights of data subjects** under the DPA which gives data subjects control over their personal data and how this data is used. The data subject has the right to give or withhold consent to processing their personal data, and the right to be informed of any processing actions. The data subject can request access to their personal data.

12. Employees/volunteers should record service user's data with the understanding that they may request to see their personal file.

13. When a Service User requests access to their data (i.e makes a Subject Access request), the Service Manager is responsible for ensuring that the relevant Team Leader and their team comply with these requests within the time limits.

14. In essence EDAS will comply with request from data subjects for information about their personal data and its processing. EDAS also needs to

- comply with a justified request from a data subject to cease processing that is likely to cause damage or distress. A

written subject access request must be dealt with promptly; 30 days from receipt of letter, or 30 days from receipt of additional information or fee if requested.

15. EDAS can refuse a data subject's access request when it would disclose information about another identifiable individual unless the third person has consented, or it is reasonable in all the circumstances to comply with the request without their consent. In practice this may mean that a service user record is redacted i.e. 'stripped' of third-party information prior to sharing with the data subject. If refusing all or any part of a request, EDAS will send the requester a written refusal notice. A refusal notice will be issued if we are either refusing to say whether we hold information at all or confirming that information is held but refusing to release it.

16. The Department of Health Guidance for Access to Health Records Requests February 2010 should be used as an additional guide, although decisions on individual cases will always be based on their particular circumstances. The ICO Subject Access Code of Practice is also available. Both documents are available to staff to provide additional understanding of EDAS 's obligations under the DPA, as well as promoting good practice.

17. **Requests for access to the records of a deceased person**

Data on a deceased person is confidential however it is not covered by the Data Protection Act but instead by the Access to Health Records Act. In deciding whether to allow access to an individual requesting information in relation to a deceased person we will need to consider any responsibility of confidentiality to that deceased person.
EDAS would also consider the rights of the applicant and data subject under the Human Rights Act, Article 8 - the right to respect for a private and family life.

The Department of Health Guidance for Access to Health Records Requests February 2010 must be consulted should a request for heath records of a deceased client be received.

If you need more information about any aspect of data protection or freedom of information, please visit the ICO website: www.ico.org.uk

Maintaining the security of the data we collect is essential. EDAS must take appropriate technical and organisational measures to protect against unauthorised or unlawful access to personal data. EDAS must take into account the nature of data and the harm to data subjects if disclosed or lost; also the impact on the EDAS reputation in the event that this happened.

Computer equipment and data should not be removed from the office without the prior approval of your line manager. As an employee you are also required to adhere to the good practice regarding the use of portable equipment and the handling of data that you work with when this data is removed from EDAS premises. (Refer Appendix 2: Guidelines for Keeping Information Safe).

If EDAS needs to transfer data outside of the EEA we would need to ensure that the receiving country has adequate protection for data, or that the data subject has given consent. Any such transfer of information must be approved by the Caldicott Guardian.

18. The Freedom of Information Act 2000

The Freedom of Information Act 2000 gives a general right of access to all types of recorded information held by public authorities and those providing services for them, subject to specific exemptions. EDAS is usually exempt; however when providing services on behalf of a public body the organisation may be obliged to disclose documents (or parts of it) to an applicant making a request under the Freedom of Information Act.

19. Monitoring

Compliance with the policies and procedures laid down in this document will be monitored by the EDAS Board of Trustees.

EDAS will periodically review and update our data security with advice from our IT providers and in line with best practice. The EDAS Board of Trustees are responsible for the monitoring, revision and updating of this document on a 3 yearly basis or sooner if the need arises

Appendix 1: Record Retention Guidelines & Recommended Retention Period

Record	Minimum Retention Period	Authority/Justification
Accident books, accident records/reports	15 years – 3 years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches the age of 21).	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR)(SI 1995/3163) as amended, and Limitation Act 1980.
Accounting records	3 years for private companies, 6 years for public limited companies	Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006
Criminal record checks and disclosures (eg a DBS certificate)	6 years following end of employment	Limitation Act 1980 – limitation for negligence (made by public etc.)
Income tax and NI returns, income tax records and correspondence with HMRC	Not less than 3 years after the end of the financial year to which they relate	The Income Tax (Employments) Regulations 1993(SI 1993/744) as amended, for example by The Income Tax (Employments) (Amendment No. 6) Regulations 1996 (SI 1996/2631)
Medical records and details of biological tests under the Control of Lead at Work Regulations	40 years from the date of the last entry	The Control of Lead at Work Regulations 1998(SI 1998/543) as amended by the Control of Lead at Work Regulations 2002 (SI 2002/2676)
Medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry	The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677)
Records of tests and examinations of control systems and protective equipment under the Control of Substances Hazardous to Health Regulations (COSHH)	5 years from the date on which the tests were carried out	The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677)
Records relating to children and young adults	Until the child/young adult reaches the age of 21	Limitation Act 1980 - limitation for negligence (made by public etc.) Conditions for processing may need to be reviewed when a child turns 13
Service User records legal action commenced	As advised by legal representatives.	Department of Health 1999 Health Service Circular 1999/053 *For the record*
Service User records – all other	8 years after the conclusion of treatment.	
Retirement Benefits Schemes – records of notifiable events, for example, relating to	6 years from the end of the scheme year in which the event took place	The Retirement Benefits Schemes (Information Powers) Regulations 1995(SI 1995/3103)

incapacity		
Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence	3 years after the end of the tax year in which the maternity period ends	The Statutory Maternity Pay (General) Regulations 1986 as amended and Maternity & Parental Leave Regulations 1999
Statutory Adoption Pay records, calculations, matching certificates and leave	3 years after the end of the tax year in which the maternity period ends	Maternity & Parental Leave Regulations 1999
Statutory Paternity Pay records, calculations and leave	3 years after the end of the tax year in which the maternity period ends	Maternity & Parental Leave Regulations 1999
Statutory Shared Parental Pay records, calculations, certificates (Mat B1s), notices and leave	3 years after the end of the tax year in which the maternity period ends	Maternity & Parental Leave Regulations 1999
Wage/salary records (also overtime, bonuses, expenses)	6 years	Taxes Management Act 1970
National minimum wage records	3 years after the end of the pay reference period following the one that the records cover	National Minimum Wage Act 1998
Records relating to working time	2 years from date on which they were made	The Working Time Regulations 1998 (SI 1998/1833)

These are recommended guidelines for the purposes of the DPA, however, if the records are currently being worked on or emergency situations, files will be kept open until the work is completed.

Appendix 2: Guidelines for Keeping Information Safe

Do –

- Read and understand EDAS 'S Policies on Data Protection, Confidentiality Policy, and Accident & Incident Reporting.
- Make passwords difficult to guess and change them regularly (use a mix of letters, numbers and symbols and a minimum of 8 digits.)
- Lock your screen when your computer is unattended (use Ctrl + Alt+ Del) & position computer terminals so that the screen cannot be seen by other people.
- Work to the EDAS clear desk policy.
- Share information on a need to know basis only and keep information to be shared to a minimum.
- Ensure that confidential documents no longer required are cross-cut shredded (or disposed of by the approved service at EDAS Head Office.)
- Retrieve printouts and faxes immediately.
- Keep filing cabinets, offices and lockers locked when not in use.
- Dispose of redundant computer and mobile computing equipment in the proper manner in accordance with EDAS policy.
- Make sure that your mobile devices are physically secure when unattended.
- Keep the information you have on your mobile device to a minimum & make sure it's backed up in accordance with EDAS policy.
- Ensure mobile devices are encrypted.
- Regularly back up the files onto the EDAS NAS drive whenever you are in the office so that a copy is held securely.
- Immediately report any actual or suspected loss, theft or unauthorised access/disclosure or suspected network security breaches.

Re

Don't -

- Remove mobile devices or data from the office without the prior approval of your line manager.
- Use your own mobile devices; they must always be approved and provided through EDAS IT Support and encrypted and in line with EDAS policy.
- Leave passwords where others can find them or share them with anyone.
- Leave paper documents with personal or sensitive information unattended or in view when off site or in a work area where they may be lost or viewed inappropriately.
- Talk about individuals in public places where you can be overheard or discuss confidential matters away from the workplace.
- Take any more confidential information off the site than is necessary for your work.
- Leave mobile devices unattended (e.g. in parked vehicles or unattended at service users' homes or other offsite premises.)