POLICY TITLE:	**Data Protection**
Policy Number:	ALE03
Applies to:	All Aspris Colleagues
Version Number:	05
Date of Issue:	02/10/2025
Date of Review:	01/10/2026
Author:	Jaz Manku, General Counsel Ananya Baishya, Data Protection Co-ordinator
Ratified by:	Katie Dorrian, Director of Governance and Quality
Responsible signatory:	Jaz Manku, General Counsel
Outcome:	This policy aims to provide clear information on the following aspects: • Confirms the responsibilities of the Legal and Data Protection Team, Group Data Protection Officer and all Aspris employees in connection with data. The processes to follow in relation to the principles as set out in the Data Protection Act 2018, as amended, regarding collection, keeping and processing of personal information. • Subject Access Requests (SARs) and what to do upon receipt of a SAR. • Information sheets for Young People and new colleagues.
Cross Reference:	AHR04.2 Disciplinary Procedures AIT02 IT Security AIT07 Printing, Photocopying, Scanning and Faxing ALE06 Confidentiality ALE03.1 Document and Data Retention ALE03.2 Management of a Data Security Breach AOP04 Incident Management, Reporting and Investigation

EQUALITY AND DIVERSITY STATEMENT

Aspris is committed to the fair treatment of all in line with the Equality Act 2010, as amended. An equality impact assessment has been completed on this policy to ensure that it can be implemented consistently regardless of any protected characteristics and all will be treated with dignity and respect.

In order to ensure that this policy is relevant and up to date, comments and suggestions for additions or amendments are sought from users of this document. To contribute towards the process of review, email AsprisGovernanceHelpdesk@Aspris.com

DATA PROTECTION

CONTENTS **Page**

1 INTRODUCTION

1.1 The UK GDPR and the Data Protection Act 2018 (together the UK data protection legislations) sets out the rules and principles in connection with processing Personal Data and Sensitive Personal Data. It places obligations on companies and individuals in how they deal with data and sets out the rights of Data Subjects. The Information Commissioner's Office oversees compliance with the law.

1.2 Aspris complies with the requirements of the UK data protection legislation. This policy should be interpreted in conjunction with the UK data protection legislation and all Codes of Practice published by the Information Commissioner's Office.

1.3 Aspris collects and processes personal information for a variety of purposes, including those connected with the employment and engagement of colleagues, the education and care of the young people we support, management of services and the reduction of risk of harm and the detection, investigation and prevention of crime. Given the core nature of the Aspris business, we give the utmost priority to young people's confidentiality.

1.4 Responsibility for compliance with the UK data protection legislations and general obligations of confidentiality lies with the Chief Executive Officer of Aspris, who provides delegated authority to senior managers within Aspris who should ensure that DPA compliant processes and procedures are in place so that the DPA principles are met and complied with at all times.

1.5 The General Counsel, in collaboration with the Data Protection Officer (DPO) possesses an expert overview of internal data protection processes and procedures. This ensures adherence to all principles outlined under the UK data protection legislation and reduces the occurrence of data breaches.

2 PURPOSE

2.1 To fulfil its contractual obligations, Aspris needs to collect and hold certain types of information about individuals and entities with whom it deals with, including employees, young people, funders and suppliers. The management of personal information must adhere to lawful practices, encompassing how it is obtained, recorded, stored, organised, retrieved, used, disclosed and ultimately destroyed. These practices apply regardless of whether the information is in physical form, stored on a computer, or recorded on any other medium. The lawful and accurate handling of personal information is an integral and significant aspect of upholding the right to confidentiality of individuals and entities with whom Aspris engages.

2.2 The UK data protection legislations set out an individual's right to confidentiality, which imposes both legal and ethical obligations on Aspris.

2.3 Colleagues are also reminded of their professional obligations of confidentiality and reference should be made to guidelines from relevant professional bodies.

2.4 Failure to comply with relevant laws may result in penalties being imposed on Aspris, and, in addition, the possibility of colleagues being investigated by their relevant professional bodies or subject to internal disciplinary action.

3 DEFINITIONS

3.1 **Data Controller** – Aspris is a Data Controller under the definition in the UK data protection legislations, because it determines the purposes for which and the manner in which any Personal Data is processed, with overall responsibility for compliance lying with the Chief Executive Officer (see 1.5).

3.2 **Data Processor** – Any person, public authority, agency or entity (other than an employee of the data controller) who processes the data on behalf of the Data Controller.

3.3 **Data Protection team** – This team is responsible for overview of Aspris' compliance with the UK data protection legislations and providing day to day guidance to colleagues on matters relating to the UK data protection legislations. Within Aspris your first point of contact should be the DPO within the Aspris Legal Team via dataprotection@aspris.com .

3.4 **Data Subject** – The individual to whom information pertains and who can directly or indirectly be identified through such information.

3.5 **Data Protection Officer (DPO)**– The Data Protection Officer (DPO) for Aspris sits within the Legal Team and is responsible for overseeing the effective management of personal and sensitive personal data processed by the Data Controller throughout the entire data lifecycle.

3.6 **Personal Data** – Any information which relates to a living individual who can be identified:

(a) Directly from the data, or;

(b) From other auxiliary information which is in the possession of or is likely to come into the possession of the Data Controller, and;

(c) Includes any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual.

3.7 **Recipient** – Any individual, public authority, agency or body to whom Personal Data are disclosed, including any third-parties to whom information is disclosed in the course of processing data for the Data Controller.

3.7.1 **Senior Information Risk Owner** – The Senior Information Risk Owner is accountable for managing information risks, overseeing the risk assessment procedures and ensuring a robust

incident reporting system specifically designed for information risks within Aspris. The Legal and Data Protection Team fulfil this role within Aspris.

3.7.2 **Sensitive Personal Data** - Personal Data consisting of information as to:

(a) Racial or ethnic origin
(b) Biometric data
(c) Genetic data
(d) Political opinions
(e) Religious beliefs or philosophical beliefs
(f) Membership of a trade union
(g) Physical or mental health or condition
(h) Sexual life
(i) Commission or alleged commission by the Data Subject of any offence, or
(j) Any proceedings for any offence committed or alleged to have been committed by the Data Subject, the disposal of such proceedings or the sentence of any court in any such proceedings.

3.8 **Third Party** – Any individual, public authority, agency or body other than the Data Subject, the Data Controller or the Data Processor(s).

3.9 **Young Person** – Any individual under the age of 18 receiving residential, support or educational services from Aspris.

4 SCOPE

4.1 This policy applies to all permanent, temporary or contracted colleagues, professionals, students and volunteers, whose personal information is being processed and who has access to the personal information of others.

5 LEGISLATIVE REQUIREMENTS

5.1 Aspris aims to ensure that all confidential information is handled in accordance with:

(a) Data Protection Act 2018 (DPA)
(b) UK GDPR
(c) The Data (Use & Access) Act 2025
(d) Privacy and Electronic Communications Regulations (PECR)
(e) Access to Health Records Act 1990 (where it still applies)
(f) Common Law Duty of Confidentiality
(g) Report of the Review of Service user Identifiable Information (1997) from the Caldicott Committee.

6 POLICY STATEMENT

6.1 Aspris is committed to complying with the UK data protection legislations to preserve:

(a) **Confidentiality:** protecting sensitive information from unauthorised disclosure
(b) **Integrity:** safeguarding the accuracy and completeness of information
(c) **Availability:** ensuring that information and vital services are available to authorised users and to ensure that any personal identifiable information received, stored, processed or transmitted is done so in a secure environment.

7 KEY PRINCIPLES

7.1 The key responsibilities that Aspris must uphold in relation to the Personal Data are summarised in the following eight points from the DPA. See section 11 for details on how Aspris puts these principles into practice.

7.2 All Aspris colleagues must ensure Personal Data is:

(a) Processed fairly, lawfully and transparently

(b) Processed for specified purposes
(c) Adequate, relevant and not excessive
(d) Accurate and up-to-date
(e) Not kept for longer than necessary
(f) Processed in accordance with the rights of Data Subjects
(g) Protected by appropriate security
(h) Not transferred outside the European Economic Area (EEA) without adequate protection

7.3 Directors can delegate tasks directly to someone holding a senior management position within their business area. On operational services, the person with overall responsibility for compliance with the UK data protection legislations is the service manager..

7.3.1 Therefore, the service manager has responsibility within their sphere of influence for the implementation of this policy and compliance with the UK data protection legislations. This includes:
(a) Arranging and facilitating local training sessions for all colleagues
(b) Liaising with the Data Protection team to enable SARs to be reviewed and responded to in a timely manner (see Appendix 1 – Subject Access Request Flowchart)
(c) Acting as an initial point of contact for all data protection issues which may arise within their sphere of responsibility.

7.4 Each member of senior management will ensure any IT system in operation within their business area is used in accordance with AIT02 IT Security, and compliant with the principles of the UK data protection legislations.

7.5 The IT Department will ensure that any new system complies with the UK data protection legislations and that all databases that require registration are registered in accordance with the requirements of the DPA.

7.6 The day-to-day responsibilities of enforcing this policy will be devolved to managers, whether on operational services or in central services. In order to effectively fulfil their roles, the Data Protection team will ensure the provision of regular training designed to remind colleagues of their professional data protection obligations and the most effective way of ensuring adequate information security and confidentiality.

8 TRAINING IMPLICATIONS

8.1 Training will take place via the Aspris Learning Lounge, or through independent trainings sessions conducted by the data protection team. Data Protection and Confidentiality e-learning modules are mandatory for all colleagues and will be completed at induction and updated annually. The IT Security e-learning module is also mandatory for all colleagues before being granted access to the Aspris network, with updates annually. This will be supplemented by further training at a level appropriate for each employee group should additional needs be highlighted during the course of ordinary business.

8.2 Colleagues at operational servicess in particular must be aware of the policies, procedures and processes around consent, record keeping, archiving, transferring and sharing personal information and steps to take if the security of Personal Data is compromised or breached.

9 GROUP COMPLIANCE

9.1 To ensure compliance with the DPA, Aspris will:
(a) Observe fully, conditions regarding the fair collection and use of Personal Data
(b) Meet its obligations to specify the purposes for which Personal Data is collected and processed
(c) Collect and process appropriate Personal Data, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements
(d) Ensure the quality of information used

(e) Apply strict checks to determine the timelines for which any Personal Data is held (in accordance with regulatory or contractual obligations)
(f) Ensure that the rights of individuals about whom information is held, are able to be fully exercised under the UK data protection legislations
(g) Take appropriate technical and organisational security measures to safeguard Personal Data
(h) Ensure that Personal Data is not transferred abroad without suitable safeguards
(i) Ensure that Personal Data shared with other organisations is only shared where appropriate and with full consideration for the Data Subject's rights

10 COLLEAGUES RESPONSIBILITIES

10.1 All colleagues are responsible for ensuring that those who do not have a legitimate need to access Personal Data are not able to do so, and to make sure that Personal Data is non-accessible to those who do not have a need to know. Colleagues must only access Personal Data if authorised and reasonably required for their role to do so or to fulfil a lawful purpose.

10.1.1 Records (whether manual or electronic) must not be left where unauthorised individuals could gain access to the information and contents of the records. All colleagues must ensure that records are kept securely at all times. Colleagues should also take care not to access files with Personal Data contained in them when working in public places; for example in a public café or on a train where members of the public are around, or a teacher in a classroom where other young people could see the Personal Data of their peers.

10.2 E-mail communications are not secure unless specific measures are taken, such as using approved encryption tools or anonymising data before sending. No Personal Data is to be transmitted outside the EEA without the permission of the Data Protection and Legal team to ensure that any such transfer is undertaken lawfully.

10.3 **All colleagues are reminded that accessing Personal Data without the permission of Aspris is a criminal offence. This does not mean that colleagues must seek specific permission in order to carry out their usual daily work duties but, for example, colleagues are not authorised to access Personal Data about a young person or another colleague unless it is a necessary part of their usual work duties or they have been authorised in advance to do so by their immediate line manager.**

11 DPA PRINCIPLES IN PRACTICE (as set out in section 7)

11.1 **Processed fairly and lawfully –** A key requirement of the DPA is to ensure that individuals (including young people and colleagues) are aware of the purposes for which their data have been obtained, the extent to which it may be processed, used or shared, their opportunity to make known any objections and who they should contact in the event that they wish to exercise their rights under the UK data protection legislations.

11.1.1 In practice, this means Aspris colleagues must:
(a) Always have legitimate grounds for collecting and using Personal Data
(b) Not use data in ways that have unjustified adverse effects on the Data Subject
(c) Be transparent about the intended use, and give individuals appropriate privacy notices when collecting their Personal Data (**ALE Form: 04** or **04A** (Easy Read) Using and Sharing Information About You, must be used for this purpose)
(d) Handle Personal Data only in ways the Data Subject would reasonably expect
(e) Make sure nothing unlawful is done with the data.

11.1.2 This is known as the 'fair processing of information'. This requires Aspris colleagues to:
(a) Be open and honest about your identity when dealing with others
(b) Tell individuals how you intend to use any Personal Data that you collect about them
(c) Usually handle their Personal Data only in ways they would expect
(d) Not use their information in ways that unjustifiably may have a negative effect on them

NB: The collection of Personal Data may sometimes be used in a manner that negatively affects an individual without this necessarily being unfair e.g. using CCTV footage from a security camera to evidence wrongdoing.

11.1.3 Where Personal Data is to be shared with other organisations, the Data Subjects should be informed that their data may be shared, so they can choose whether or not to enter into a relationship with Aspris. For example, there may be certain instances where a Third Party may require access to records e.g. National Regulators, Placing Authority Inspectors, Independent Persons visiting a home under Regulations 44 (England) / Regulation 8 (Wales): see ACS Form 45 – Access to Records for Inspection: Children's Homes.

11.1.4 Unless one of the specific exemptions applies (see section 18), individuals should generally be able to choose whether or not their Personal Data is disclosed to a Third Party.

11.1.5 In order for Aspris to comply with the DPA principles, all young people **must** be given the information leaflet **ALE Form: 04 or 04A** Using and Sharing Information About You and new colleagues will receive **ALE Form: 04D** Data Protection and Young Person Information. If any new information is acquired that does not align with the general descriptions outlined in those documents, it is imperative to notify the young person or their family about the existence of that data, its intended purposes of collection, processing, usage and the proposed duration of data retention.

NB: On request documents will be provided in an accessible format to meet the requirements of **Disability Discrimination Act (DDA). Copies can be obtained in large print, audio and Braille, or in a different language by submitting a request to the Aspris Marketing Team at marketing@aspris.com.**

11.1.6 **Processed for specified purpose –** Personal Data must only be collected for specified purposes, and must not be further processed in any manner incompatible with those purposes. In practice this means that colleagues must:

(a) Be clear from the outset about why data is/are being collected and what they are collected for;
(b) Comply with the DPA's fair processing requirements – including the duty to give the information notices to individuals when collecting their Personal Data; and
(c) Ensure that if you need to use or disclose the Personal Data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair.

11.1.7 If you need to use or disclose Personal Data for a purpose that was not initially contemplated at the time of collection, is necessary to assess whether it would be unfair due to being beyond what the individual would have reasonably expected or have an unjustified adverse effect on them. In practice, you would need to obtain prior consent from the individual to use or disclose Personal Data for a purpose that is supplementary to, or different from, the original purpose for which consent was obtained .

11.2 **Accurate and up to date** – Personal Data shall be adequate, relevant to the purpose or purposes for which they are processed. In practice, it means you should ensure that:

(a) You take all reasonable steps to ensure that the Personal Data you hold about individuals is not incorrect or misleading;
(b) You do not hold more information than you need for that purpose; and
(c) the Personal Data you hold is updated and the most correct version of information.

11.2.1 Personal Data is inaccurate if it is incorrect or misleading as to any matter of fact. Therefore, there is a requirement to identify the minimum amount of Personal Data that is needed to properly fulfil the purpose for which the data is/are collected. This could include a requirement to collect more Personal Data than was originally anticipated. However, you should not hold Personal Data on the off chance that it might be useful in the future except in relation to a potential but foreseeable event e.g. Blood Group of a young person or colleague may be collected to deal with a potential medical emergency.

11.2.2 Personal Data should not be collected or processed if it is insufficient for its intended process e.g. CCTV images that are poor quality, thereby making identification difficult.

11.2.3 When handling Sensitive Personal Data, it is crucial to limit the collection and retention of information to the required minimum.

11.2.4 To comply with this principle you must:
(a) Take reasonable steps to ensure the accuracy of all Personal Data you obtain
(b) Ensure that the source of any Personal Data is clear
(c) Carefully consider any challenges to the accuracy of information
(d) Consider whether it is necessary to update the information.

11.2.5 It is acceptable to keep records of events that happened in error, provided those records are not misleading about the facts. You may need to add a note to a record to clarify that a mistake happened.

11.2.6 Personal Data should be kept up to date where the information is used for a purpose that relies on it remaining current e.g. a young person's change of address.

11.2.7 It may be impractical to check the accuracy of Personal Data that someone else provides. You will not be considered to have breached this principle as long as:
(a) You have accurately recorded the information provided by the individual concerned, or by a Third Party
(b) You have taken reasonable steps in the circumstances to ensure accuracy of the information
(c) If the individual challenges the accuracy of the information, this is clear to those accessing it.

11.2.8 If the information source is someone you know to be reliable, or is a well known organisation, it will usually be reasonable to assume they have given you accurate information, unless common sense suggests that there may be a mistake.

11.2.9 If a young person challenges the accuracy of information held about them you should consider whether the information is accurate and, if it is not, you should delete or correct such information after being satisfied that the information was recorded incorrectly. (In the case of heath records, the NMC guidance on record keeping in The Code must be followed).

11.2.10 An expression of an opinion about an individual is classed as their Personal Data. So when recording information about an individual, you should record whether it is an opinion, and, where appropriate, whose opinion it is.

11.3 **Not kept longer than necessary -** Personal Data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes. In practice this means that you will need to:
(a) Review the retention period of Personal Data
(b) Consider the purpose or purposes for which the information for in deciding whether (and for how long) to retain it
(c) Securely delete information that is no longer needed to fulfil the purpose or purposes
(d) Update, archive or securely delete information when the purpose is fulfilled.

11.3.1 Discarding Personal Data too soon would likely disadvantage Aspris and cause inconvenience to the Data Subject the information relates to.

11.3.2 Personal Data will need to be retained longer in some cases than others. The appropriate retention period is likely to depend on the following:
(a) What the information is used for
(b) The relationship between the Aspris and the individual
(c) Any legal or regulatory requirements
(d) Agreed industry practice.

11.3.3 To determine the retention period of data refer to ALE03.1 (Document and Data Retention) and ALE Form 05 (Retention Periods for documents and data amends), which determine Aspris divisional policies on record keeping. Further advice can be sought from the Data Protection team by emailing dataprotection@aspris.com .

11.4 **Processed in accordance with the rights of the data subject -** Personal Data shall be processed in accordance with the data protection legislations, with due regard to the rights of the Data Subject at all times. Individuals have a right to:

(a) Access a copy of the information comprised of their Personal Data (see section 12 Subject Access Requests (SARs)),
(b) Object to processing that is likely to cause or is causing damage or distress to them,
(c) Prevent processing for direct marketing,
(d) Object to decisions being taken by automated means,
(e) In certain circumstances, to have inaccurate data rectified, blocked, erased or destroyed, and
(f) Claim compensation for damages caused by a breach to their rights and freedom under the data protection legislations.

11.4.1 **An individual's right to object to processing** – An individual has a right to object to processing their data only if it causes unwarranted and substantial damage or distress. If it does, they have a right to require an organisation to stop (or not to begin) the processing in question. An individual who wants to exercise this right has to put the objection in writing and state what they require you to do to avoid causing damage (financial loss or physical harm) or distress (emotional or mental pain). The extent to which you must comply is limited to:

(a) The individual can only object to you processing their Personal Data
(b) Processing the Personal Data must cause unwarranted and substantial damage or distress

11.4.2 An individual has no right to object where:

(a) The processing is necessary:
  i) In relation to a contract that they have legally entered into
  ii) Because the individual has asked for something to be done so they can enter into a contract
(b) The processing is necessary because of a legal obligation that applies to you
(c) The processing is necessary to protect the individual's vital interests.

11.4.2.1 An individual can object to the processing of any information regarding themselves. This needs to be considered on a case-by-case basis where the individual must give specific reasons why they are objecting to processing of their data. Unless there is an absolute right, we (Aspris) can refuse to comply, if:

- we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

(further information - Right to object | ICO)

11.4.3 **The right to prevent direct marketing** – Individuals have the right to prevent their Personal Data being processed for direct marketing purposes. An individual can, at any time, by informing in writing, object or withdraw previously given consent to stop (or not begin) using their Personal Data for direct marketing. This can be done by directly emailing the Marketing Team at marketing@aspris.com. Aspris is obligated to promptly cease processing Personal Data for direct marketing. Compliance requires the termination of all electronic communications within 28 days and postal communications within 2 months.

11.4.3.1 However, Aspris will not use personal details of young people for marketing of any services that we provide. It will use geographic and personal records for internal marketing research, but not in any way outside Aspris.

11.4.4 **Rights relating to inaccurate personal data** – Where any information is inaccurate, an individual has a right to apply to the court for an order to rectify, block, erase or destroy the

inaccurate information. Where the information in question has been provided by a Third Party, Aspris will not be considered to be in breach as long as:

(a) The information provided by the Third Party has been recorded correctly
(b) Aspris has taken reasonable steps to ensure the accuracy of the information
(c) If the individual has challenged the accuracy of the information, this is clear to anyone who accesses it.

11.4.5 This right also applies to Personal Data that contains an expression of opinion based on inaccurate Personal Data.

11.4.6 **The right to compensation** – If an individual suffers damage due to a breach of the data protection legislations caused by Aspris, they are entitled to claim damages. The data protection legislations allows Aspris to defend a claim on the basis that all reasonable care in the circumstances was taken to avoid the breach. An individual who has suffered financial loss as a result of a breach is likely to be entitled to compensation.

11.4.6.1 An individual who has suffered distress alone will not usually be sufficient to entitle them to compensation. There is no fixed criteria for determining the appropriate level of compensation for an individual; rather, such determinations are made on a case-by-case basis. Upon receiving a request for compensation, it is advisable to promptly seek guidance from the Data Protection team.

11.5 **Protected by Appropriate Security -** Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to Personal Data. In practice, Aspris must have appropriate security to prevent the Personal Data that we hold from being accidentally or deliberately compromised. (Also refer to ALE06 Confidentiality and AIT07 Printing, Photocopying, Scanning and Faxing, and divisional Record keeping policies with regard to security of records).

11.5.1 To meet this requirement Aspris has deployed appropriate physical and technical security, which is backed up by robust policies and procedures.

11.5.2 Aspris has the following systems in place to ensure that data is held securely:

(a) All hard-copy personnel files must be held in secure lockable cabinets in the HR departments or by the People Services Team (HR). The cabinets need to be locked when the offices are unoccupied
(b) Any personal information transmitted electronically or transferred using electronic media must be encrypted using approved software in accordance with AIT02 IT Security
(c) Colleagues must not send young person or colleague data to their own personal email address or devices
(d) Colleagues who have access to Personal Data (young person or other colleague) must handle such information in accordance with this policy. Failure to do so may result in disciplinary action in accordance with AHR04.2 Disciplinary Procedures.
(e) The IT Network is protected by technical measures including firewalls and anti-virus software
(f) Laptops, tablets and other devices are encrypted
(g) All mobile devices are password protected with the ability to remote wipe if the device has been lost
(h) All electronic data is held securely within systems and can only be created, amended or read by colleagues authorised to do so
(i) All electronic data held in applications is backed up on a daily basis and replicated at our Disaster Recovery Centre
(j) Copies of electronic young person or colleague records must not be made e.g. on flash drives or memory sticks or any other device
(k) Hard copy young person or colleague records may not be taken off the services premises (including printouts of electronic records) without the express permission of the service manager
(l) The IT Network is protected from unauthorised external access using a Sonicwall Firewall and an SSL Sonicwall Aventail appliance which restricts connections to authorised systems on the internal network. Only users with a valid user account on the SSL Sonicwall Aventail appliance will be granted access. The password policy applied automatically by the network

requires regular changing of users' passwords and the use of complex passwords; refer to AIT02 IT Security regarding further password requirements

11.6 **Transfer Outside the European Economic Area –** Personal Data will not be transferred outside the EEA unless that country ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data. Alternatively, the data protection team must be informed of such requirement of data transfers to inadequate jurisdictions for appropriate measures to be implemented to facilitate such transfers. No data should be transferred without the prior involvement of the Data Protection team.

11.6.1 The lawful transfer of data overseas requires the recipient country to adhere to and/or have similar data protection laws to the United Kingdom (UK). Currently such provisions only apply to members of the EEA. Placing data on the internet will involve transfers to countries outside the UK; seeking software support from companies outside the UK may also involve data transfer outside the EEA.

11.6.2 Transferring Personal Data also includes information written on paper.

11.6.3 Before making a restricted transfer to an inadequate jurisdiction, you should consider whether you can achieve your aims without actually sending personal data. For example, if the data is made anonymous so that it is never possible to identify individuals from it, then in this case the restrictions do not apply, and a transfer can be made outside the EEA.

11.6.4 If there is a need to send Personal Data to countries outside of the EEA, this must be discussed with the Data Protection team to ascertain the levels of protection for the information and how these can be assured.

11.6.5 Aspris may transfer Personal Data overseas under the following conditions:

(a) With the express consent of the individual, conveyed clearly, freely, and with the option of withdrawal. Consent will not be valid if the individual has no choice but to give their consent. The individual must be informed and must have understood, and acknowledged the reasons for the transfer, the countries involved and the associated risks.
(b) Where it is necessary to carry out a contract that the individual has entered into with Aspris
(c) Where it is necessary for reasons of substantial public interest. Substantial public interest is most likely to be relevant in the prevention and detection of crime, national security and collecting tax. The public interest must be that of the UK and not the country the Personal Data is transferred to
(d) Where it is necessary to protect the vital interests of the individual. This relates to matters of life and death
(e) In connection with legal proceedings, to obtain legal advice or to establish, exercise or defend legal rights. The legal proceedings do not have to involve Aspris or the individual as a party.

12 SUBJECT ACCESS REQUESTS (SARs)

12.1 Individuals have a right to have a copy of personal information that Aspris hold on them. In addition to a copy of the information, the Data Subject is also entitled to:

(a) A description of the purposes for which the data is being processed
(b) The Recipients or classes of Recipients to whom the data may be disclosed
(c) Any information available to the Data Controller as to the source of the data.

NB: If any of the information is not immediately or commonly identifiable, perhaps due to a code or abbreviation, an explanation must be provided.

12.2 All colleagues should familiarise themselves with what a SAR is and what forms it could take. SARs should be sent to dataprotection@aspris.com immediately on receipt.

12.2.1 In addition, independent special schools in Scotland are subject to the Freedom of Information (Scotland) Act from September 2016. As such, requests for information under this Act must be dealt with in accordance with the statutory framework. If you work at a school in Scotland and

received a request for information under the Freedom of Information (Scotland) Act please liaise with the Data Protection team immediately by contacting dataprotection@aspris.com .

12.3 SARs notified to the Data Protection team will be logged and provide guidance as to how to respond to it if applicable. A SAR can be made in any format (letter, email or fax, verbally or even by posting on social media). The information does not have to be provided until the identity of the applicant has been verified. (See **Appendix 1 -** Subject Access Request Flowchart).

12.4 All such requests must be responded to within 28 calendar days of receiving the request. This may be extended for an additional two months under specific circumstances, as deemed necessary and determined by the data protection team. The deadlines for responses to SARs must be adhered to. If we do not, we could be liable to a complaint being made to the Information Commissioner's Office and a fine being issued for non-compliance.

12.5 Colleagues must verify the identity of the applicant before sending them information. Requests may be received from a Third Party on behalf of an individual e.g. solicitor, relative. In these cases, you need to be satisfied that the Third Party has written authority to act on behalf of the Data Subject (refer to paragraph 17.8).

12.6 Where Aspris reasonably requires further information in order to be satisfied about the identity of the person making the request, the applicant must be informed of this in writing as soon as possible. The request does not have to be complied with until the further information is supplied. The Data Protection team will provide more guidance in these circumstances if needed.

12.7 With regard to information, other than that contained within a young person's record, the right of access is only to information held by Aspris in an electronic form or, in a file that is sufficiently indexed to enable any personal information to be located within it relatively easily (properly known as a relevant filing system).

12.8 For the avoidance of doubt a young person does have a right of access to his/her records, subject to exceptions dealt with below.

12.8.1 Where Aspris cannot comply with the request without disclosing information that would identify the Third Party, then that information should be redacted from the information shared with the requestor unless:

(a) The Third Party has expressly consented in writing to the disclosure of the information to the applicant

(b) It is reasonable in all the circumstances to comply with the request without the consent of the Third Party. What is reasonable in all the circumstances requires consideration to be given to the following factors:

i) Any duty of confidentiality owed to the Third Party;

ii) Any steps taken by Aspris with a view to seeking the consent of the Third Party;

iii) Whether the Third Party is capable of giving consent; and

iv) Any express refusal of consent by the other individual.

(c) The circumstances in paragraph 17.5 apply.

12.8.2 Where information about a Third Party will be disclosed then approval of the Data Protection team must be obtained in advance.

12.9 The information to which an applicant has a right of access must be supplied in permanent form (at the applicant's request), which could mean a copy of the relevant document or creating a new document containing the information or an electronic document. Usually, information will be provided in the form of a copy document with deletion of any information to which the application is not entitled.

12.10 **Requests for information about young persons -** Even though a young person may not fully understand the implications of subject access rights, it is important to recognise that data pertaining to them constitutes their Personal Data and does not belong to a parent or guardian. Consequently, the young person holds the right to access the information held about them, even

though in the case of the young person these rights are likely to be exercised by those with parental responsibility. When addressing a SAR for information concerning a young person, it is vital to consider whether the young person is mature enough to understand their rights. If Aspris is confident that the young person understands their rights, it is advisable to gain consent from and respond to the young person rather than a parent. In such instances, it is imperative to fully explain this course of action to the parent and seek advice from the Data Protection team in these circumstances.

12.10.1 When considering cases you should take into account, among other things:
(a) The young persons level of maturity and their ability to make decisions
(b) The nature of the Personal Data
(c) Any court orders relating to parental access or responsibility that may apply
(d) Any duty of confidence owed to the young person
(e) Any consequences of allowing those with parental responsibility access to the young person's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment
(f) Any detriment to the young person if individuals with parental responsibility cannot access the information
(g) Any views the young person has on whether their parents should have access to information about them.

12.10.2 In Scotland, the law presumes that a young person aged 12 years or more has the capacity to make a SAR. The presumption does not apply in England, Wales but it does indicate an approach that may be considered reasonable in most cases, subject to consideration on a case-by-case basis.

12.11 **Data that includes information about other people** – responding to a SAR may involve providing information that relates both to the individual making the request and to another individual. The DPA says that you do not have to comply with a request if to do so would mean disclosing information about another individual who can be identified from that information, except where:
(a) The other individual has consented to the disclosure
or
(b) It is reasonable in all circumstances to comply with the request without the individual's consent.

12.12 **Repeated or unreasonable requests** – The UK data protection legislations do not limit the number of SARs that an individual can make to an organisation. You do not have to comply with an identical or similar request to one you have already dealt with, unless a reasonable interval has elapsed. To consider whether a request has been made at a reasonable interval you should consider the following:
(a) Whether the data is particularly sensitive
(b) If the processing is likely to cause detriment to the individual
(c) Whether the data is unlikely to have changed between requests.

12.13 All SARs must be sent to the Data Protection team (dataprotection@aspris.com) to be managed and recorded in a central log. This central log will be reviewed periodically to consider whether changes are required to internal training and support or to this policy.

13 INDIVIDUAL'S CONSENT

13.1 Colleagues must always ensure that an individual is aware of what is going to happen to the personal information that they provide to us. For example, a young person and/or their parents or carers should be made aware when information is going to be passed to their general practitioner or to a professional outside Aspris to enable the provision of further care/treatment/support/education. Where any disclosure is going to take place to an individual or organisation outside Aspris, in a context not connected with the care of a young person or routine colleague administration matters (such as payroll or disclosure to the Inland Revenue), then the individual's written consent must be obtained in advance of any such disclosure.

13.2 There are circumstances under which it is sufficient to inform an individual of the purposes for which their data are collected and processed and thereby gain their implied consent. In most cases however, their 'explicit consent' must be obtained.

13.3 An individual's consent to processing will not be required, provided that:

(a) The individual is already aware, in general terms, of the particular purpose for which the information is to be used
and
(b) The processing is necessary or required by law
and
(c) The processing is consistent with any other applicable law, for example, the law of confidentiality
(d) Disclosure is justified in the public interest
(e) The data is anonymised.

13.3.1 For example, for personal information other than Sensitive Personal Data, processing may take place where it is necessary for the performance of a contract to which the young person or colleague is a party (for example, an employment contract). This makes practical sense as it demonstrates that there is no need to obtain a colleague's permission every time information is sent to payroll, for example. The processing is also permissible where it is necessary for the business purposes of Aspris although such processing would not take place where it was unwarranted in any particular case if it would prejudice the rights or some other legitimate interest of the individual concerned.

13.4 In relation to Sensitive Personal Data, explicit consent to processing must be obtained from the young person where they have capacity. This means that the individual has been fully informed about the uses of the data and any potential disclosures and their active agreement has been secured. As a matter of policy, this agreement must be recorded in writing. However, consent is not always required, but in addition to the circumstances set out in paragraph 13.3 above, the following criteria need to be met:

(a) The processing must be necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on Aspris in connection with employment.
(b) The processing is necessary for medical purposes and is undertaken by a health professional or another Aspris colleague who will owe a similar duty of confidentiality to the individual. Medical purposes include the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

13.5 This allows the day-to-day functioning of Aspris to take place without requiring an individual's specific agreement each time their personal information is passed between those responsible for their care/treatment/support or education.

13.6 There are other circumstances where processing without consent is permissible. However, in all other cases or where there is any concern about whether personal information is being processed lawfully, the advice of the Data Protection team must be sought.

13.7 Consideration should be given to the processing of any Personal Data under any new systems implemented by Aspris, and input must be sought from both the IT, Legal and the Data Protection teams.

14 DISCLOSURE OF PERSONAL INFORMATION

14.1 Personal information will not be disclosed outside Aspris unless it is consistent with this policy and the fair processing of information (see paragraph 11.1), there is a statutory obligation to do so, it is otherwise lawful or the individual has given his/her consent to the disclosure.

14.2 In giving consent the individual must be informed of the extent of any disclosure and its implications. In all cases no more information will be disclosed than is necessary to achieve the purpose behind the disclosure.

14.3 The duty to obtain consent is not absolute, but can only be overridden if the Data Controller can justify disclosure on the grounds that the public interest in maintaining confidentiality is outweighed by the public interest in making the disclosure (for example in order to protect the vital interests of the data subjects or another person, or for the prevention and detection of crime). Before making any such disclosure, the proposed disclosure should be discussed with Data Protection team and in the case of doubt about the legality of disclosure, legal advice should be sought.

14.4 There are statutory obligations to disclose, i.e. information must always be disclosed if required by legislation/statute or court order e.g. notifications of communicable diseases, abortion, substance misuse, etc.

14.5 There are statutory restrictions on the disclosure of information relating to HIV and AIDS, other sexually transmitted diseases, assisted conception and assisted abortion.

14.6 Public Interest Disclosure Act 1998, as amended is designed to protect colleagues who make certain disclosures of information in the public interest by amending the Employment Rights Act 1996, as amended. It offers protection against reprisals/victimisation of colleagues who disclose information (usually to their employer) which, in the reasonable belief of the worker making the disclosure, tends to show the occurrence or likely occurrence of:

(a) A criminal offence
(b) A person's failure to comply with any legal obligation
(c) A miscarriage of justice
(d) The health and safety of an individual being endangered
(e) Damage to the environment.

14.7 It also includes information tending to show any matter relating to paragraph 14.3 that has been, is being or is likely to be deliberately concealed. Such disclosures are defined as qualified disclosures for the purposes of the Public Interest Disclosure Act 1998. The DPA makes provision for it to be overridden if there are public interest reasons why data protection should not apply, but any disclosure must be justifiable and recorded.

14.8 There may be circumstances in which Personal Data may need to be used in responding to a major incident or dealing with a risk to public health. A decision to use information relating to individual people would only be taken by the incident control team if judged to be in the public interest to do so.

14.9 Requests for information in relation to a young person or an Aspris colleague from a UK police force would normally be refused. However, under Section 29(3) of the DPA, Aspris is permitted to make such disclosures in the public interest, at our discretion for the prevention or detection of crime. Nevertheless, this is not an obligation to disclose the data. The request must be in writing, justifying the grounds for disclosure, and submitted to the appropriate service manager or specialist director. All such requests should be forwarded to the Data Protection team for review.

14.10 Where information relating to a young person is to be used in research, the Data Subject should be informed about the intended use of this information before disclosure takes place. This applies irrespective of whether or not the results are to be made available to the young person in a form that identifies them (with their consent).

14.11 Disclosures of information about deceased persons will be handled as SARs under the surviving part of the Access to Records Act (see **Appendix 1** – Subject Access Request Flowchart).

14.12 In exceptional circumstances requests for information in relation to a young person or an Aspris colleague from the Home Office may be subject to the immigration exemption or Part 3 of the DPA 2018. All such requests must be forwarded to the Data Protection team for review (dataprotection@aspris.com)

15 ANONYMISING INFORMATION

15.1 The removal of personal details alone may be sufficient to protect an individual's identity when disclosing information. If anonymisation is to be relied upon as the condition for disclosure without consent, it requires the removal of **all** information that could allow identification of a living individual.

15.2 For some uses of data, the retention of an identification number or other tracking code may be acceptable if recipients of the data do not have access to the 'key' to trace the identity of the young person. Such anonymisation may, with appropriate safeguards, be sufficient to allow use without express consent. It is good practice to inform people that their information may be used anonymously for audit purposes.

NB – Particular care must be taken not to breach any confidentiality or data protection requirements when returning property to a young person's relative(s) on discharge or death to ensure that all documents containing Personal Data within the property are reviewed.

16 SHARING INFORMATION BETWEEN ORGANISATIONS

16.1 Young person's information should only be shared between organisations that have adopted an appropriate policy.

16.2 The principles governing the sharing of personal information are essentially the same as those governing its use within an organisation. The difference is in the extent to which control measures need to be taken and made explicit. The responsibilities for protecting the confidentiality of young person's information extend to any individuals and agencies to whom information is passed. Furthermore, such information may only be used for the specific purpose for which it is shared. The organisation releasing (or disclosing) the information is responsible for ensuring that the Recipient keeps it secure and confidential and uses it only for the agreed purpose(s). If you are unsure whether it is appropriate to share information with another organisation (such as a Local Authority), please contact dataprotection@aspris.com for guidance.

16.3 Personal Data may need to be shared with Independent Visitors as part of their Regulation 44 (or other regional equivalent) visits. In such cases, ACS Form 45 should be completed and signed as set out in section 11 of this policy.

16.4 **Business Information –** All information concerning the operations of Aspris and all companies within it, is confidential. Information relating to the business may only be disclosed when specifically authorised by Directors and protected by appropriate legal documents (usually non-disclosure agreements). Aspris has copyright and design rights on publications, assessment formats, forms and data systems. These may not be published or shared with any other organisations without the express written permission of the Directors. The Legal Team must be contacted if further clarification on the disclosure of commercial documents not containing personal information is required.

17 DATA PROCESSORS

17.1 Where personal information is to be processed on behalf of Aspris the following requirements must be met:

(a) There must be a written contract;
(b) The contract must provide that the data processor will only act on instructions from Aspris;
(c) The contract must provide that the data processor will comply with the requirements for appropriate, technical and organisational measures which must be taken against unauthorised or unlawful processing of personal data and against accidental loss of destruction of, or damage to, personal data.

17.2 Unless a Data Processor can demonstrate the appropriate security measures referred to above and unless a contractual guarantee is provided that the compliance with those measures will be in place then Aspris will not enter into the contract with that Data Processor.

17.3 **Provision of Health Information -** There are additional provisions with regard to personal information about someone's physical or mental health or condition. It is important to note that a young person has a right of access to the information contained in his/her health records, subject to certain exemptions. These special provisions apply not just to health records but to information wherever it is recorded about someone's health or condition.

17.4 There is no right of access to health information to the extent to which it would be likely to cause serious harm to the physical or mental health or condition of the young person or any other persons (including the health care professionals concerned with the person's treatment). It is the responsibility of the health professional who is currently or was most recently responsible for the clinical care of their young person in relation to those particular records, to make the decision on this issue. Where no such health professional is available, then it must be a health professional who has the necessary experience and qualifications to advise on this issue and in these circumstances, it will be determined in consultation with the Director of Governance and Risk and the DPO.

17.5 Aspris will not release health information to an applicant falling in the following groups:

(a) Information provided by the person in the expectation that it would not be disclosed to the applicant

(b) Information obtained as a result of any examination or investigation to which the person consented in the expectation that the information would not be disclosed to the applicant

(c) Information which the person has expressly indicated should not be disclosed to the applicant.

17.6 This proviso does not apply to the extent that the request relates to information, which Aspris is satisfied has previously been seen by the applicant or is already within the knowledge of the applicant, perhaps because he or she provided the information. Furthermore, if in the previous six months the appropriate health professional has already given an opinion that the exemption applies then there is no need to re-consult unless it is reasonable in the circumstances to do so.

17.7 The restrictions on the identification of third parties when disclosing health information does not apply to identification of a health professional who has compiled or contributed to a young person's health record or has been involved in the care of the young person in his or her capacity as a health professional.

17.8 **Request for Data by a Third Party -** No one other than the young person has a right to his or her personal information (apart from the points raised above about young persons and adults without capacity). However, others may be appointed to act as agents for the service user, such as solicitors or relatives. In such circumstances, written authorisation from the data subject (or the individual with legal responsibility for them if they are under 13 or do not have capacity) must be obtained prior to the release of any personal information to the agent. **ALE Form 04B** Authority from Data Subject for Access to Personal Sensitive Information is available for this purpose, and please seek advice from the Data Protection team (dataprotection@aspris.com). There are also instances where access to records may be required by National Regulators, Placing Authority Inspectors, Independent Persons visiting a home under Regulations 44 (England) / Regulation 8 (Wales): see ACS Form 45 – Access to Records for Inspection: Children's Homes.

17.8.1 Aspris must be satisfied that the young person is aware of what he or she is consenting to in these circumstances. In cases of doubt, the Data Protection team must be consulted. If the young person lacks capacity to consent but is over the age of 18 years, written authorisation by way of a Power of Attorney granted in relation to the young person's affairs or an order of the Court of Protection would be required. Copies of such written authorisation should be always kept on file at the service along with full details of the request for data and the response to it. As indicated in paragraph 14.6 above, in rare cases, a request for information may be received from a UK police force if they are investigating a serious crime. There are circumstances where it would be lawful to provide the information, but no such disclosure must take place without consulting with the Data Protection team.

17.9 Enquiries from relatives and friends must be handled in accordance with the wishes (with consent) of the young person, taking care to positively identify the enquirer and their relationship to the young person. If in doubt, Aspris will not share any personal details with the person making the

enquiries. Aspris colleagues with access to confidential information **must not** pass on any information to their relatives or friends or seek to find out details about themselves. Personal details of young people, their diagnosed conditions and their treatment must not be disclosed otherwise than in accordance with this policy. No information shall be passed on for personal or commercial gain. Disciplinary action will be taken against colleagues if confidential information is disclosed in these circumstances.

17.10 Personal Data should never be inputted into any kind of artificial intelligence (AI) programme, system, software or any other medium for any reason.

18 EXEMPTIONS

18.1 There are some exemptions in the UK data protection legislations to accommodate special circumstances in respect of disclosure and non-disclosure. Specific advice should always be sought from the Aspris Legal Team and the Data Protection team before making any disclosures under an exemption to the UK data protection legislations.

18.1.1 It is sometimes appropriate to disclose Personal Data for certain purposes to do with criminal justice or the taxation systems. In particular, where the processing of Personal Data could assist in:
(a) The prevention or detection of crime
(b) The capture or prosecution of offenders
(c) The assessment or collection of tax or duty.

18.1.2 Personal Data processed for any of the above purposes is exempt from:
(a) Aspris' duty to comply with Data Protection Principle 1, but not including the duty to satisfy one or more of the conditions for processing;
and
(b) An individual's right to make a SAR. This is to ensure that any investigation is not prejudiced by disclosing the information to the Data Subject.

18.1.3 The UK data protection legislations provide an exemption for processing data in connection with regulatory activities. This exemption is not available to all organisations and it applies only to bodies that perform public regulatory functions concerned with:
(a) Protecting members of the public from dishonesty, malpractice, incompetence or seriously improper conduct or in connection with health and safety
(b) Protecting charities
(c) Fair competition in business.

18.1.3.1 For the exemption to apply, those functions must also be
(a) Conferred by or under an enactment
(b) Functions of the Crown, a Minister or government department
(c) Any other public function exercised in the public interest.

18.1.4 Where an organisation is obliged by or under an enactment to make information available (by publishing) to the public, Personal Data that is included in that information is exempt from:
(a) The subject information provisions;
(b) The non-disclosure provisions;
(c) The organisations duty to comply with Data Protection Principle 4, Accuracy
(d) An individual's right in certain circumstances to have inaccurate personal information rectified, blocked or erased or destroyed.

18.2 **Disclosures Required by Law -** Personal Data is exempt from non-disclosure if you are required to disclose it:
(a) By or under a UK enactment
(b) By any rule of common law
(c) By an order of a court or tribunal in any jurisdiction.

18.2.1 In these circumstances the legal obligation overrides any objection that individuals may have. Always seek advice from the Aspris Legal Team if you receive a Court Order or other request to disclose information under this exemption.

18.3 **Legal Advice or Proceedings -** Personal Data is exempt from non-disclosure where the disclosure of the data is necessary:
(a) For or in connection with any legal proceedings (including prospective legal proceedings)
(b) For obtaining legal advice
(c) For establishing, exercising or defending legal rights.

18.3.1 Aspris is not required to disclose Personal Data in response to a Third Party. Aspris can choose whether or not to apply the exemption and the Third Party may seek to obtain a Court Order to require the disclosure of the data concerned. In the event that a Court Order is received, Aspris is required to comply with its provisions and advice should be sought immediately from the Aspris Legal Team.

18.4 **Confidential References -** Personal Data is exempt from an individual's right of SAR if it comprises a confidential reference that an organisation gives in connection with education, training or employment, appointing office holders, or providing services**. The exemption does not apply for references that an organisation receives.**

18.5 **Management Information -** Personal Data that is processed for management forecasting or management planning in respect of an individual is exempt as it would be likely to prejudice the business or other activity of the organisation. Example: If a business was planning a reorganisation then the business would be exempt from having to disclose the plans to an individual.

18.6 **Negotiations -** Personal Data that consists of a record of an organisation's intentions in negotiations with an individual does not have to be disclosed as it could prejudice the outcome. Example: The resolution of a personal injury claim, in which the insurance company contests the severity of the claim and the proposed settlement amount.

18.7 There are other exemptions which are not likely to be relevant to your professional work at Aspris. These are in relation to:
(a) Data stored by an individual only for the purposes of their personal, family or household affairs
(b) National security and the armed forces
(c) Personal Data that is processed only for journalistic, literary or artistic purposes
(d) Personal Data that is processed only for research, statistical or historical purposes
(e) Personal Data relating to an individual's physical or mental health. This applies only in certain circumstances and only if granting a subject access would be likely to cause serious harm to the physical or mental health of the individual or someone else
(f) Personal Data that consists of educational records or relates to social work
(g) Personal Data relating to human fertilisation and embryology, adoption records and reports, statements of a young persons special educational needs and parental order records and reports
(h) Personal Data processed for, or in connection with, a corporate finance service involving price–sensitive information
(i) Examination marks and personal Data contained in examination scripts
(j) Personal Data processed for the purposes of making judicial, Crown, or Ministerial appointments or for conferring honours.

19 AUDITS

19.1 An audit of Data Protection processes will be conducted by all departments/services twice a year as a minimum. Guidance should be obtained from the Data Protection team.

20 REFERENCES

20.1 Data Protection Act 2018 - See Website: http://www.ico.gov.uk
Access to Health Records Act 1990
Employment Rights Act 1996
Public Interest Disclosure Act 1998
Caldicott, F (2013) Information: To share or not to share? The Information Governance Review
DH (2013) Information: To share or not to share? Government response to the Caldicott Review
HSCIC (2013) A Guide to Confidentiality in Health and Social Care: Treating confidential information with respect
ICO (2014) Subject Access Code of Practice: Dealing with requests from individuals for personal information
General Data Protection Regulation (UK GDPR) (Regulation (EU) 2016/679)

APPENDIX 1 – Subject Access Request Flowchart
APPENDIX 2 – Information Sheet for New Colleagues (**ALE Form: 04D**)

Associated forms:

ALE Form: 04	Using and Sharing Information About You
ALE Form: 04A	Using and Sharing Information About You – Easy Read
ALE Form: 04B	Authority from Data Subject for Access to Personal Sensitive Information
ALE Form: 04D	Data Protection and Young Person Information
ALE Form: 07	Email Acceptance and Text Message Declaration
ALE Form: 07B	Email Acceptance and Text Message Declaration – Education & Children's Services
ACS Form: 45	Access to Records for Inspection: Children's Homes

Also see divisional forms and letters associated with Record Keeping and Access to Records

APPENDIX 1

SUBJECT ACCESS REQUEST FLOWCHART

Request for Personal Information Received
Determine whether this request should be treated as a routine enquiry or as a Subject Access Request

YES
Any enquiry that asks to information that we hold about the person making the request can be construed as a subject access request.
e.g. "Please send me a copy of my personnel records"
"I have the right to see all the invoices issued to me for the last three years. Please send me copies"
"I am a solicitor acting on behalf of my young person and I request a copy of the medical records. An appropriate letter of authority is enclosed"

NO
In many cases there will be no need to treat the request as a Subject Access Request. If you would usually deal with the request in the normal course of business, then do so.
e.g. "Can you tell me what my hospital number is please?
I have a query on my last invoice, can you let me know what the amount was for?

Handle the query as part of your usual course of business following any Confidentiality or Data Protection policies as normal.
There is no need to notify the Data Protection team of these queries.

Check the requesters' identity.
If the requester is a third party, check that they have the authority of the person that the information is about, **before** you provide any information and obtain consent.

(For young people who do not have capacity to consent, refer to AOP05 Mental Capacity).

Other necessary Information
You will need to ask the requester for any other information you need to find the records they want promptly as these may be in several different places. You may have quite a wide search if they can't narrow down their request. Please note, the requester is not obligated to supply further information, but we must still comply with the request.

Notify the Data Protection team

Please forward all requests to dataprotection@aspris.com.

A central log of all SARs will be kept by the data protection team and they will provide advice and guidance on how to respond to the request.

28 Days Response time
Aspris operates a 28-calendar day response time to comply with all SARs. This commences when the initial request is received or when identification/evidence of

Collate all records requested

Personal Data can be stored in many different locations, such as electronic care notes, physical files, and letter and email correspondence. A full and complete search should be completed to locate any and all data that has been requested.

NO
If you hold no personal information about the individual you **must** tell them this in writing within the 28 day timeframe.

YES
Routine changes to the information can be made in the normal course of business, but changes MUST not be made as a result of receiving the request, even if inaccurate or embarrassing information is found within the record.

References to Third Parties
Aspris must not supply this information unless the other people mentioned have given their consent or it is reasonable to supply information without their consent. Check the records for any third-party information and mark it for redaction. Follow our Guide to Redaction for assistance with this.

Exempt Information

There may be circumstances in which Aspris is not obliged to supply certain information. Some of the most important exemptions apply to:

- Crime prevention and detection
- Negotiations with the requester
- Management forecasts
- Confidential references given by you (but not to you)
- Information used for research, historical or statistical purposes
- Information covered by legal professional privilege e.g. the consultant can withhold medical information if disclosure to the requester would cause a significant danger to the requester or to a third party

If **ALL** the information that you hold is exempt you can reply by telling them that you do not hold any information that you are required to reveal.

If some of the information is exempt then this does not need to be included in the response.

Complex terms or codes

The information may include abbreviations, medical or technical terms that the individual will not understand. You must make sure that these are explained so that the information can be understood. The best way is to provide a glossary.

Preparing the Information to be sent

A copy of the information should be supplied in a permanent form as requested by the individual concerned.

Remember: Aspris has an obligation to comply with the request within 28 days starting from when you receive all the information necessary to deal with the request. An extension for a request can only be made in exceptional circumstances (*e.g. when documents requested are dated pre-GDPR, any document that is difficult to locate within the 28 days tenure, etc.***). Individuals can complain to the Information Commissioners' Office or apply to a court if Aspris does not respond within this time limit.**

The requested information can then be delivered either:

- By hand to the requester in person (after verifying their identity) by the service; or
- Sent by registered post to an agreed address with a return address on the parcel by the service or data protection team (*as agreed*); or
- Send via secure and encrypted email such, and sign in using your usual username and password by the service or data protection team (*as agreed*).

Please check with the requester which format (digital/electronic or physical) they would prefer.

A copy of what has been sent is stored by the Data Protection Team within a secure drive.

Notify the Data Protection Team that the request has been completed.

APPENDIX 2 – Information sheet for new colleagues (**ALE Form: 04D**)

DATA PROTECTION AND YOUNG PERSON INFORMATION

This document must be read in conjunction with the Aspris policy [ALE03 Data Protection]

Personal information will be obtained from and about young people while using the services provided by Aspris. Some of the information will be of an administrative nature such as their name, address and contact details. Other information may be about their mental and physical health. Generally speaking, information obtained from a young person will be held in confidence by Aspris. Individual colleagues may also owe legal and ethical obligations of confidentiality to the young people we support when information is provided to them. Personal information, whether it is confidential or not, must also be dealt with in accordance with the Data Protection Act. Consultants and therapists may also maintain their own independent records of contact with young persons. In such cases it is the clinician's responsibility to inform the young person and comply with his/her own legal obligations.

As a general rule, confidential information must not be processed without the young person's explicit consent, unless the processing can be justified in the substantial public interest or there is some other legal basis for using the information, such as a Court order or statutory obligation. Under the Data Protection Act, provided the young person has been informed in general terms of the purposes for which their information is going to be used (as well as the other criteria set out in ALE03 Data Protection) then personal information may be processed. However, personal information from which the young person might be identified should not be used for the purposes of any kind of research without the young person's explicit consent. In order that young people are sufficiently informed about the purposes to which their information will be put, the information sheet ALE Form: 04 will be supplied to each new young person upon contracting services from Aspris.

There are many circumstances where confidential information about young people is shared between professionals in the course of providing care/treatment/support/education for them. It is not necessary to obtain a young person's explicit consent on each occasion provided that the young person is generally aware that information is going to be passed in this way. For example, it is not necessary to obtain a young person's explicit consent every time a professional writes to a general practitioner, local authority or other stakeholder involved in the young person's care. However, young people must be aware that such exchanges are likely to take place and if a young person withdrew their consent for such correspondence, then that should be respected. Another example would be information provided to a young person's funding organisation in order for Aspris to obtain reimbursement.

If the young person has been assessed to lack capacity to consent, then a 'Best Interests' decision must be in place instead.

In compiling and processing young person's records the principles set out in the policy ALE03 Data Protection must be followed. The following additional points should be followed (based on the Caldicott principles for health and social care records):

(a) Truly anonymised information should be used wherever it can be. For example, for the purposes of audit or administration.
(b) If it is not possible to use truly anonymised information and there is a requirement to be able to "track back" then rather than using information that can directly identify a young person, a unique identifier should be used, for example, a young person number.
(c) In general terms and wherever possible and practicable, a young person's explicit consent should be obtained for the passage of information. The less directly connected with the young person's care the passage of information is, the more the requirement. In any case, where information is passed without explicit consent, you must be able to justify why that consent has not been obtained.
(d) Justify the purpose(s) of using the young person's data.
(e) Use the minimum person-identifiable information necessary for the purpose.

(f) Access to person-identifiable information must be on a need to know basis.
(g) Colleagues must be aware of their responsibilities and obligations with regard to confidentiality.
(h) Colleagues must understand and comply with the law as set out in this policy.

If a young person refuses their explicit consent to a particular use or disclosure of information, then it is the responsibility of the colleague in charge of their care/treatment/support/education to ensure that they have been provided with full information as to the consequences of their refusal. Such circumstances must be recorded in writing together with the explanation that has been given and the young person should be asked to initial the note to acknowledge that they have received the information and understood it and the consequences of their refusal.

If a circumstance arises where any young person information is to be transferred outside Aspris in circumstances that are not covered by part of ALE03 Data Protection, then before any such transfer of information takes place the Data Protection team must be consulted.

Young people have a right of access to their personal information and/or health/social care/education records.

A young person's personal information and records will be retained in accordance with the policy ALE03 Data Protection and divisional record keeping policies. All records for destruction will be disposed of securely.

(After reading, you should give a signed copy to your service HR Administrator or send it to the central People Services Team, so it can kept with your HR records).

Signed…… Name…….. Date……..