POLICY TITLE:	**Confidentiality**
Policy Number:	ALE06
Version Number:	02
Date of Issue:	06/03/2024
Date of Review:	05/03/2027
Policy Owner:	Laura Neubauer, Director of Legal Services
Ratified by:	Jane Stone, Director of Governance and Risk
Responsible Signatory:	Laura Neubauer, Director of Legal Services
Outcome:	This policy: • Aims to ensure that young persons, their families or representatives and colleagues are assured of confidentiality. • Details the delegation of officers such as the Caldicott Guardian. • Provides details on the safe and secure transfer of all confidential information used across Aspris. • Aims to ensure all colleagues comply with the requirements of the Data Protection Act when dealing with young person or colleague personal information.
Cross Reference:	AIT02 IT Security AIT07 Printing, Photocopying, Scanning and Faxing AIT11 Information Transfers ALE03 Data Protection ALE05 Service User Information/Interview Requests from Police or Other External Agencies AOP04 Incident Management, Reporting and Investigation AOP05 Mental Capacity AOP06 Safeguarding Children AOP06A Safeguarding Children in Residential Care AOP06B Safeguarding Children in Education - Wales AOP08 Safeguarding Adults AOP08A Safeguarding Adults - Wales AOP21 Whistleblowing (Protected Disclosure)

EQUALITY AND DIVERSITY STATEMENT

Aspris is committed to the fair treatment of all in line with the Equality Act 2010. 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.

This policy covers all parts of Aspris Services – The Care and Education Divisions; Central services and our Fostering service. For the Fostering service and the 2 operational divisions, there are local procedures that relate to some of these policies, where necessary.

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.

CONFIDENTIALITY

1 INTRODUCTION

1.1 All colleagues are required to protect confidential information concerning young people and other colleagues obtained in the course of their work, as well as any commercially sensitive information.

1.2 Personal data is covered by the Data Protection Act 2018 and any breaches of confidentiality will be treated as an incident. Therefore this policy must be read in conjunction with:
(a) ALE03 Data Protection;
(b) AIT07 Printing, Photocopying, Scanning and Faxing;
(c) AOP04 Incident Management, Reporting and Investigation;

2 AIMS

2.1 Young people, children, students, their family or representatives and colleagues have the right to be assured that information given in confidence will only be used for the purpose for which it was given and will not be released to others without their permission. The death of a young person does not give the right to break confidentiality.

2.2 Confidentiality is to be respected at all times and general confidential information must only be shared to enhance care and only with the young person's consent. Confidentiality may only be broken in exceptional circumstances and may only occur after very careful consideration by senior management (refer to ALE03 Data Protection).

2.3 Colleagues should be aware of the over-riding duty to breach confidentiality where there is a potential risk of harm to the young person, another colleague or members of the public. Safeguarding matters are likely to fall into this category. (Refer to AOP06 Safeguarding Children and AOP08 Safeguarding Adults).

3 TRAINING

3.1 All colleagues who have access to confidential information, whether commercial information or personal information relating to either the young people Aspris supports or colleagues, will receive training on how to share confidential information, for both induction and refresher e-Learning modules courses via the Aspris Learning Lounge appropriate to their role.

4 CORPORATE GOVERNANCE

4.1 All colleagues, including contractors, must be subject to strict confidentiality obligations in their contracts. A confidentiality statement is included on all emails being sent to external recipients and is included on electronic records.

4.2 If there are any question as to whether confidential information, whether commercial or relating to individuals, can be disclosed outside of Aspris then advice should be sought from the Legal and/or IT teams.

4.3 Any commercially sensitive information (for example financial information) must be sent by an appropriately secure method of communication.

5 SECURITY

5.1 IT systems and policies should offer robust arrangements for managing access and sharing of young person's identifying information according to agreed management protocols. This will include written documentation, IT system information and any confidential information kept on individual business systems such as mobile phones/laptops and any other media processing

devices. All colleagues will read the policy, AIT02 IT Security, before they are given an access login to the Aspris network.

5.1.1 'Systems' also includes images captured on surveillance cameras such as CCTV, or digital cameras used for taking identification images on admission.

5.2 Colleagues must ensure that confidential hard copy records are kept in locked storage facilities and not accessible to unauthorised people at any time.

6 PROVIDING INFORMATION

6.1 It is important that the young person (and their family or representatives, if applicable) understands that some confidential information may be made available to others involved in the delivery of their care.

6.2 The young person (and their family or representatives, if applicable) is to be made aware with whom the confidential information will be shared and for what purpose it will be shared.

6.3 As far as is reasonable, confidential information is to be kept in strict professional confidence and be used only for the purposes for which the information was given.

6.4 Other than in the limited circumstances stated in paragraphs 6.5(b) and 6.5(c) below, explicit consent from the young person is always required before confidential information is disclosed. If the young person does not have the capacity to give consent, a best interests decision must be in place prior to sharing of any confidential information.

6.5 Disclosure of confidential information is permitted:
(a) With the consent of the young person.
(b) Without the consent of the young person when the disclosure is required by law or by order of a court.
(c) Without the consent of the young person when the disclosure is considered to be necessary in the public interest.

6.6 Disclosing information in the public interest means the interest of an individual or groups of individuals or of society as a whole, and would, for example, cover matters such as serious crime, drug trafficking or other activities, which places others at serious risk.

6.7 Colleagues are responsible and accountable for any decision they make to release confidential information.

6.8 Colleagues are not to deliberately breach confidentiality other than in the exceptional circumstances noted in paragraphs 6.5(b) and 6.5(c).

6.9 Any enquiries from the press, radio or television will be referred immediately to the site/service/departmental manager and advice sought from the Aspris communications team.

6.10 The private addresses or phone numbers of individuals should not be included in young person's documentation or reports, unless it is expressly required for the function of that documentation.

6.11 Failure to comply with this policy will result in disciplinary action.

7 CONFIDENTIALITY AND THE YOUNG PERSON

7.1 Data subjects have the same data protection rights regardless of age. Both the BMA and GMC expressly state that the duty of confidentiality owed to a young person is as great as the duty owed to any other person.

7.1.1 If a child or young person does not agree to disclosure of confidential information there are still circumstances in which disclose can take place:
(a) When there is an overriding public interest in the disclosure.
(b) When disclosure is in the best interests of a child or young person who does not have the maturity or understanding to make a decision about disclosure
(c) When disclosure is required by law.

7.1.2 In respect of 7.1(b) above, young people aged 16-17, and younger people under 16 who are Gillick competent are considered to have the maturity to understand the decision regarding disclosure and are entitled to have their confidence respected.

7.2 A child can be regarded as Gillick competent if a doctor concludes that he/she has the capacity to make the decision that needs to be made at that particular time and has sufficient understanding and intelligence to be capable of making up his/her own mind. (Established in Gillick v West Norfolk and Wisbeach Area Health Authority (1986)).

7.3 In safeguarding cases it sharing information essential to safeguard a child's welfare would satisfy the "overriding public interest" threshold.

8 CALDICOTT PRINCIPLES

8.1 Dame Fiona Caldicott led an in depth Information Governance Review in 2013 of the well-established Caldicott Principles for the maintaining the confidentiality of Health and Social Care records, leading to an updated set of seven principles (see **Appendix 1**).

8.2 The review also lays out a set of five confidentiality rules which must be followed by all colleagues having access to personal confidential data:
(a) Confidential information about children and young people should be treated confidentially and respectfully.
(b) Members of a care team should share confidential information when it is needed for the safe effective care of a child or young person.
(c) Information that is shared for the benefit of the community should be anonymised.
(d) An individual's right to object to the sharing of confidential information about them should be respected.
(e) Organisations should put policies, procedures and systems in place to ensure that the confidentiality rules are followed.

9 DELEGATION OF OFFICERS

9.1 Colleagues should be advised to seek assistance from their manager or the Aspris Data Protection Team where necessary. Typical examples of such situations are:
(a) A request from the police for access to service user information (also refer to ALE05 Young Person Information/Interview Requests from Police or Other External Agencies).
(b) Requests from young persons to delete their records.
(c) An actual or alleged breach of confidentiality.

9.2 Refer to ALE03 Data Protection for information regarding the Group Data Protection Officer for Aspris.

10 COLLEAGUE CONFIDENTIALITY

10.1 Colleagues have a responsibility to ensure confidentiality when dealing with professional issues or complaints relating to another colleague.

10.2 Managers should ensure sensitivity and confidentiality to the colleague involved in any issue or complaint, where possible and appropriate.

10.3 The private addresses or phone numbers of colleagues should not be included in young person documentation or reports.

11 SECURE & SAFE TRANSFER OF CONFIDENTIAL INFORMATION (SAFE HAVEN)

11.1 The term 'Safe Haven' describes the administrative arrangements to safeguard the confidential transfer of young person's' identifiable information between organisations or sites. It covers data held on:
(a) Fax machines.
(b) Answerphones.
(c) Photocopiers, printers.
(d) Computers, laptops, mobile phones.
(e) Message books.
(f) Post trays, including unopened post.
(g) Visitor books.
(h) Dictation equipment.

11.1.1 Reference should be made to AIT11 Information Transfers when transferring data electronically.

11.2 When information is disclosed by a designated safe-haven point to an equivalent point in another organisation, colleagues can be confident that agreed protocols will govern the use of the information from that point on.

11.3 Responsibility for maintaining the confidentiality of young persons' identifiable information lies with the site/service manager or the departmental manager for central service functions. Individual colleagues are responsible for ensuring that the procedures are always applied when transferring confidential data between organisations.

11.4 **Printers, Photocopiers, Scanners and Fax Machines** - Refer to AIT07 Printing, Photocopying, Scanning and Faxing for guidance on maintaining confidentiality of this equipment.

11.5 **Post** - Post should be opened in an area away from young people and visitors. Post in and out trays must be sited away from the general public and stored in an area with controlled access.

11.6 **Message Books, Appointment Books etc. -** Written records must be sited away from the general public and at the end of each session must be stored in a secure location.

11.7 **Computers, Email and Mobile Phones** - young person's identifiable information must not be sent by email. However, there will occasionally be instances where it is appropriate to use a young person's name rather than initials in email communication, for example when corresponding with family.

11.8 Computer screens must be away from the sight of visitors and the general public. This includes views from ground floor windows. Users of computer systems must log out of all application systems before leaving a PC unattended. Refer to AIT02 IT Security.

11.8.1 The use of personal mobile phones or cameras to take photographs of young people is not permitted.

11.9 **Other Electronic Media** - Dictation equipment containing personal information should always be kept in a locked area when not in use. They should be cleared of all dictation when the communication has been completed. There must be an area available for colleagues to use the phone away from public areas and photocopiers/printers should be sited in areas where there is no access for the public and young people.

12 FILMING, PHOTOGRAPHY OR VIDEO

12.1 Unless expressly authorised in advance by a site leader or other senior manager for purposes strictly connected with work, colleagues are not permitted to take pictures, film or record footage (using phones or other recording equipment) of young people or other colleagues whilst at work.

12.1.1 This also applies to covert filming. If a colleague has concerns about the care or treatment of a service user, this must be reported to line management in accordance with AOP21 Whistleblowing (Protected Disclosure).

12.2 Anyone found taking pictures or recording footage of young people or colleagues either overtly or covertly, without the express permission of senior management for a legitimate work purpose (such as supervision or training) will be dismissed for gross misconduct. The matter is likely to be notified to the police, the Information Commissioner's Office (ICO) and relevant regulatory, safeguarding and professional bodies.

13 USING GENUINE CASE STUDIES

13.1 All information that relates to a living person is subject to the requirements of the Data Protection Act (refer to ALE03 Data Protection). These guidelines must be followed if case studies of young persons or colleagues containing such information are used externally for publicity, marketing, tendering or for any other reason.

13.2 All materials intended for external use/general publication/public media must be approved in writing by the central Communications team before use. The Communications team will check that appropriate consents and safeguards are in place to ensure that the requirements of the Data Protection Act are not breached, for example:

(a) Articles do not contain the young person's/colleague's real name
(b) Young People and/or colleagues have consented to the use of photographs. (If the young person lacks capacity to consent and consent has not been provide by their parent, photographs of them must not be used)
(c) Other details about colleagues and/or young people do not identify the subject as a specific person
(d) No reference is made to the location of any residential home for safeguarding purposes.

13.3 Case studies for restricted external use (e.g. tenders and proposals) should be sourced in the first instance from In the Loop or from the Communications team, as these will already have been checked to make sure the appropriate consents or safeguards are in place.

14 REFERENCES

14.1 **Legislation**

Data Protection Act 2018
Health and Social Care Act 2012, Section 265

14.2 **Guidance**

DH (2003) Confidentiality: NHS Code of Practice
DH (2013) Information: To share or not to share. Government response to the Caldicott Review
Health and Social Care Information Centre (2013) A Guide to Confidentiality in Health and Social Care: Treating confidential information with respect
NMC (2015) The Code: Professional standards of practice and behaviour for nurses and midwives (updated 2018)
A Manual for Caldicott Guardians - (https://www.ukcgc.uk/caldicott-guardians-manual)
DHSSPSNI (2011) Residential Care Homes Minimum Standards
DHSSPSNI (2015) Care Standards for Nursing Homes
Scottish Government (2018) Health and Social Care Standards: My support, my life

Regulated Services (Service Providers and Responsible Individuals) (Wales) (Amendment) Regulations 2019
Gillick v West Norfolk and Wisbech Area Health Authority [1985] 3 All ER 402

Appendix 1 – The Caldicott Principles

TO SHARE OR NOT TO SHARE
The Caldicott Principles

(Text originally adapted for Priory from 'A Guide to Confidentiality in Health and Social Care (HSCIC) 2013, amended to refer to Aspris)

1. **Justify the purpose(s)** – Every proposed use or transfer of personal confidential data within or from an Aspris site should be clearly defined scrutinised and documented, with continuing uses regularly reviewed, by the person in charge of the site.

2. **Don't use personal confidential data unless it is absolutely necessary** – Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for service users to be identified should be considered at each stage of satisfying the purpose(s)

3. **Use the minimum necessary personal confidential data** – Where use of personal confidential data is considered to be essential the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out

4. **Access to personal confidential data should be on a strict need to know basis** – Only those individuals who need access to personal confidential data should have access to it, and then should only have access to the data items that then need to see.

5. **Everyone with access to personal confidential data should be aware of their responsibilities** – Action should be taken to ensure that colleagues handling personal confidential data, (which means all colleagues, whether clinical, non-clinical or office colleagues) are made fully aware of their responsibilities and obligations to respect service user confidentiality.

6. **Comply with the Law** – Every use of personal confidential data must be lawful. The Caldicott Guardian is responsible for ensuring that Aspris complies with legal requirements, and it is the responsibility of every colleague to ensure that they comply with the requirements set out in Aspris policy, and use the systems and processes put in place correctly.

7. **The duty to share information can be as important as the duty to protect service user confidentiality** – All Aspris colleagues should have the confidence to share information in the best interests of their service users with the framework set out by these principles. They are supported by the policies of the regulatory and professional bodies and by Aspris policies.