This policy applies to all personal data held by or on our behalf. It includes manual/paper records and personal data that is electronically processed by computer systems or other means such as CCTV systems.

Data Protection and Confidentiality Policy

Document management

Directorate	People and Governance
Policy sponsor	Chief People and Governance Officer
Policy owner	Director of Governance, Compliance and Regulation
Policy author	Assistant Data Protection Officer

Review process

Approval route	Directors Team – Executive Leadership Team – Audit and Risk Committee - Board
Approved by	Executive Leadership Team
Approval date	28 November 2024
Effective	17 December 2024
Review Frequency	Annual
Review date	15 October 2026
Version number	1.1

CONTENTS

Part 2

Policy introduction

Scope

This policy supports Amplius' values and is a commitment to improving lives and supporting colleagues by explaining the legislative reason for the robust management of Amplius' personal data and supports the effective running of Amplius' business in line with data governance and controls.

The policy sets out the principles and legal requirements under UK data protection law that Amplius must satisfy when obtaining, handling, processing, transporting or storing personal data in the course of its operations and activities, including customer, supplier and colleague data. This policy complies with the UK GDPR and the Data Protection Act 2018, and it sets out what Amplius will do to ensure confidentiality is appropriately maintained.

The term Amplius incorporates all member companies and subsidiaries.

The policy applies to Colleagues, Board Members, Consultants, Contractors, and third parties engaged in services on behalf of Amplius.

This policy may be updated at any time. Questions about the policy, the UK GDPR, or concerns about non-compliance should be directed to the Data Protection Team at data.protection@amplius.co.uk

The policy does not form part of any colleague's contract of employment and the policy may be amended at any time.

Caldicott Guardian Principles:

Amplius operates within the common law duty of confidentiality. It ensures adherence to the Caldicott Guardian Principles when collecting and sharing information in delivering its services.

The policy does not form part of any colleague’s contract of employment and the policy may be amended at any time.

Part 3

Policy details

Data Protection Principles

Personal data is defined as data which relates to a living individual which:

- Directly identifies a person (e.g., name, address, or contact information).
- Indirectly identifies a person when combined with other data (e.g., a unique ID number, IP address or an expression of opinion in respect of a person)

Amplius will follow these data protection principles:

1. **Lawful, Fair, and Transparent Processing:** Personal data will be processed lawfully, fairly, and transparently.
2. **Purpose Limitation:** Data will only be collected for specific, explicit, and legitimate purposes and not further processed in ways incompatible with those purposes.
3. **Data Minimisation:** Personal data collected will be adequate, relevant, and limited to what is necessary for the purposes it serves.
4. **Accuracy:** Data will be accurate and kept up to date as needed. Inaccurate data will be erased or corrected without delay.
5. **Storage Limitation:** Data will not be stored in an identifiable form for longer than necessary for the purposes it serves.
6. **Security:** Data will be processed securely, protecting it against unauthorised or unlawful processing and against accidental loss, destruction, or damage through appropriate technical and organisational measures.

How We Process and Manage Data

1.1 Data Minimisation

We will strive to use the minimum of personal data in processing activities and will periodically review the relevance of the information we collect. Internal colleagues and data process owners are responsible for ensuring that no un-necessary, irrelevant or unjustifiable personal data is kept, collected or created.

1.2 Data Accuracy

We recognise that the accuracy of data is important, and that some data is more important to keep up to date than others. Internal colleagues guided by data process owners will keep data as accurate and up to date as possible, in particular data which would have a detrimental impact on data subjects if it were deemed inaccurate. Personal data that is assumed inaccurate will be dealt with appropriately through erasure or anonymisation.

1.3 Data Retention

Personal data will not be retained for any longer than is necessary and for the purposes for which it is collected. Appropriate measures will be taken at the end of the data's useful life such as erasure to ensure this. Internal data process owners will be responsible for determining the retention period for the personal data their teams handle and for updating the Record of Processing Activities when processing has ceased.

1.4 Information Security

Information security is contained within the ICT use and security guidelines document this gives detailed assurance that any personal data is held securely and confidentially.

1.5 Record Keeping and Accountability

In order to fulfil Amplius' responsibility to be able to demonstrate compliance with Data Protection legislation we will maintain records of Amplius' data processing activities that Amplius controls, undertakes or otherwise commissions as required by the Data Protection legislation and specifically those required in Article 30 of the UK GDPR.

1.6 Consent

Where required, consent will be obtained, maintained and reviewed in accordance with the UK GDPR offering individuals real choice and control. We will only rely on consent when:

- it has been explicitly and freely given by the data subject when they agree to the processing of personal data relating to them.
- the consent was given through a statement made by the data subject or by a clear affirmative action undertaken by them.
- we can demonstrate that the data subject has been fully informed about the data processing arrangements and we are able to prove that we have obtained valid consent.

We will set a specific timeframe for how often consent needs to be renewed, such as annually, to make sure consent is current and valid for data processing.

We will ensure that we have processes in place to make it easy for individuals to withdraw their consent at any time. Additionally, we will inform individuals how to exercise their right to withdraw consent.

1.7 Personal/ Sensitive Data Breaches

We maintain a Data Breach Reporting Procedure and ensure that all colleagues and those with access to personal data are aware of it. All colleagues and individuals with access to personal data must report all personal data breaches to the Data Protection team as set out in the Data Breach Reporting Procedure as soon as they become aware of a breach.

Any breach of this policy must be reported immediately to the Data Protection team. All breaches will be thoroughly investigated to ensure we learn from them and take appropriate action, which could ultimately lead to disciplinary action.

1.8 Data Processing Activities

We reserve the right to contract out data processing activities or operations involving the processing of personal data in the interests of business efficiency and effectiveness. No third-party data processors will be appointed who are unable to provide satisfactory assurances that they will handle personal data in accordance with the Data Protection legislation.

1.9 Data Sharing, Disclosure and Transfer

We only share personal data with third parties where there is a legal basis for doing so and this data sharing is necessary for specified purposes. No sharing is permitted to occur without an 'Information Sharing Agreement' being in place. These agreements must be approved by a member of the Data Protection Team and stored in a central register.

IT Security guidelines provide information and approved methods of transferring personal data. If these guidelines are not followed, then disciplinary action may be taken.

1.10 Subject Access Requests (SARs)

Individuals have the right to access their personal data and any person may request access to the data we hold about them. Such requests should be immediately passed to the Data Protection team for action. After successful ID verification and request clarification we are required to respond to these requests within a calendar month.

To protect the privacy of third parties, any third-party personal information within the data will be redacted before it is shared.

However, access may be limited in certain cases where exemptions apply. These exemptions could include situations where providing access would negatively impact the rights and freedoms of others or where other legal restrictions apply.

Unless there are exceptional circumstances, data subject access requests (SARs) are typically provided free of charge. A 'reasonable fee' may be charged to cover administrative costs if a request is manifestly unfounded or excessive, or if an individual requests further copies of their data.

1.11 Sharing Personal Data Outside the UK

We will neither transfer, process nor permit personal data outside the UK without the conditions laid down in the Data Protection legislation being met. This will ensure that the level of protection of personal data is not undermined.

1.12 Risk Assessments and Impact Assessments

We foster a culture of privacy by design; when we are planning new processes or projects that involve the processing of personal data, we will carry out a Data Protection Impact Assessment (DPIA) or a Legitimate Interest Assessment (LIAs) or a Risk Assessment. This is to ensure that potential risks to individuals can be identified and addressed at the beginning of the implementation stage and data protection good practice can be built into our processes.

The Data Protection team will provide training and support on DPIAs, LIAs and Risk Assessments including completing a DPIA checklist to see if one is necessary.

We retain copies of DPIAs which are linked to our ROPA.

The operational risk register includes a risk that covers data protection risks and is reviewed quarterly.

1.13 Children's Data

We take extra precautions when processing personal or sensitive data related to children under the age of thirteen. This includes checking the age of children to determine if parental consent is required. We also ensure that any disclosures are made directly to the child, and we carefully handle privacy information and respond to information rights requests in a way that is appropriate for their age and understanding.

1.14 Training and Awareness

We will ensure all our colleagues who engage in processing personal data are provided with appropriate training in this and our other associated policies and procedures. We also undertake data protection awareness campaigns routinely to keep data protection front of mind. Mandatory refresher training is provided to all staff annually.

1.15 Audit and Compliance Checking

We will undertake periodic compliance checks to test whether this policy is being adhered to and to test the effectiveness of control measures. Records will be kept of all such audits and compliance checks including corrective actions taken.

Data Subjects Rights and Requests

Amplius will uphold the rights of individuals to access and retain control over their personal data held by us.

Amplius complies with:

The right to be informed - by ensuring individuals are informed of the reasons for processing their data in a clear, transparent and easily accessible form and informing them of all their rights.

The right of access - by ensuring that individuals are aware of their right to obtain confirmation that their data is being processed; access to copies of their personal data and other information such as a privacy notice and how to execute this right.

The right to rectification - by correcting personal data that is found to be inaccurate. We advise data subjects on how to inform us that their data is inaccurate. Inaccuracies with be rectified without undue delay.

The right to erasure - we advise data subjects of their right to request the deletion or removal of personal data where processing is no longer required or justified. Unless Amplius demonstrates legitimate grounds for the processing, which override this right.

The right to restrict processing - we restrict processing when a valid request is received by a data subject and inform individuals of how to exercise this right. Unless Amplius demonstrates legitimate grounds for the processing, which override this right.

The right to data portability - by allowing, where possible, data to be transferred to a similar organisation in a machine-readable format.

The right to object - by stopping processing personal data, unless we can demonstrate legitimate grounds for the processing, which override the interest, rights and freedoms of an individual, or the processing is for the establishment, exercise or defence of legal claims.

This does not stop anyone wishing to make a complaint about the way we handle their personal data. This can be done by following our Complaints procedure. If a customer or colleague still has concerns, they can contact the Information Commissioners Office direct on their website ico.org.uk.

Confidentiality

All personal information held by Amplius will be managed in line with our legal requirements for confidentiality. To ensure individuals know how their information may be used and shared Amplius has set out clear information on its literature and in the privacy notice.

Caldicott Guardian

Organisations that process personal, sensitive data for the provision of health and social care, must appoint a Caldicott Guardian to oversee and provide 'moral guidance' on how confidential data is used and shared.

Amplius operates in adherence with the 8 Caldicott Guardian Principles. These principles are as follows:

Principle 1: Justify the purpose(s) for using confidential information. Principle 2: Use confidential information only when it is necessary. Principle 3: Use the minimum necessary confidential information.

Principle 4: Access to confidential information should be on a strict need-to-know basis.

Principle 5: Everyone with access to confidential information should be aware of their responsibilities.

Principle 6: Comply with the law.

Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality.

Principle 8: Inform patients and service users about how their confidential information is used.

The Caldicott Principles work alongside the Data Protection Principles. They are of most relevance to situations within the health and social care setting where it is necessary to share information for the provision of 'direct care' to a service user.

In line with both Data Protection legislation and the Caldicott Principles, Amplius will keep customers informed of how their health information will be used and shared, including their rights under NHS 'National Opt-Out'.

The Caldicott Guardian is the Director of Independent Living.

Equality, diversity and inclusion

Amplius will ensure that it considers the potential impact of processing on Equality, Diversity and Inclusion in its data processing activities.

Additional needs (addressing vulnerabilities)

Amplius understands that some of our customers and service users may be vulnerable for various reasons. Our policies will consider the recommendations made by the Housing Ombudsman and other regulatory bodies regarding vulnerabilities. Amplius will take a proactive approach when making decisions about customers or service users and, where possible, will tailor our services to meet their needs and support vulnerable individuals.

Part 4

Compliance and administration

Legal and regulatory compliance

This policy fully complies with Amplius' legal and regulatory obligations.

- UK General Data Protection Regulation (UK GDPR)
- Retained General Data Protection Regulations (EU) 2016/679 (EU GDPR)
- Data Protection Act 2018 (DPA2018)
- Caldicott Principles (2020 version)
- Privacy and Electronic Communications Regulations 2003 PECR
- Data Use and Access Act 2025.

This list is not exhaustive, and policy authors will undertake thorough research and/or seek professional advice to ensure that Amplius meets its obligations and complies with the current and relevant legislation and regulations.

Evaluation, review and performance monitoring

This policy will be reviewed on a Annual basis to ensure that it remains fit for purpose. A policy review may also be required earlier, in response to internal or external changes for example changes in legislation. Prompt and effective action will be taken where improvements are identified.

The Board will receive an annual report which provides assurance in respect of data protection, data processing and data governance.

The Audit and Risk Committee receive information in respect of data breaches, this may in turn be escalated to the Board should this be deemed appropriate.

Amplius' Privacy Notice will be reviewed where there is a change in the law and will be reviewed annually.

Related policies

- CCTV and Surveillance Policy
- Safeguarding Adults and Children Policy

Part 5

Appendices

A. Associated documents – Internal procedural document, colleague use only

- Privacy Notice
- Record of Processing Activities - LG
- CCTV Procedure - LG
- Data Breach Procedure - LG
- Data Retention Schedule - LG
- Subject Access Request Procedure.

Part 6

Changelog

Amended date	Summary of changes	Version №
18/12/2025	Board reviewed the policy and approved the extension of the policy review date to 15/10/2026 in line with the policy management framework cycle.	1.1