The Anthony Seddon Fund
Supporting mental wellbeing in our community

Document Control	
Title:	**Data Protection & Confidentiality Policy**
Version:	**6**
Reference Number:	**HR-PP-IG-01**
Scope:	
All trustees, employees, volunteers, and other connected individuals of **The Anthony Seddon Fund.**	
Purpose:	
The purpose of this policy is to provide guidance on Data Protection and Confidentiality, ensuring all those performing duties on behalf of **The Anthony Seddon Fund** are aware of their responsibilities concerning confidential information. This policy sets out the approach to be taken by the charity to ensure a robust Data Protection and Confidentiality framework is in place.	
Supersedes:	
HR-PP-IG-01 – Data Protection & Confidentiality Policy – V5	
Version Changes:	
• Added a new Section 4 – Legal and Regulatory Framework, referencing UK GDPR, DPA 2018, and related legislation. • Incorporated a note on the Caldicott Principles for context. • Updated document reference to reflect revised naming convention. • Updated Section 17 – Review to reflect the charity's new tiered policy review cycle.	
Next Review Date:	June 2026
Review Tier:	Tier 1

Contents

1. Introduction

The Anthony Seddon Fund recognises that in the course of its work, trustees, staff, and volunteers gain access to confidential and personal information about individuals and organisations. With the advent of the **General Data Protection Regulation (GDPR) and the Data Protection Act 2018**, it is crucial that all such information is handled with the highest standard of privacy and security.

The charity is committed to safeguarding the personal information it holds and ensuring compliance with legal obligations. The GDPR enhances privacy rights and enforces stricter handling procedures. Therefore, our policies and practices are designed to ensure that all personal data is handled lawfully, fairly, and transparently.

Through this policy, we set out the measures and responsibilities necessary to uphold these standards, ensuring all those involved in processing personal data within the charity understand their roles and are equipped to protect the integrity and confidentiality of the data entrusted to us.

This policy covers the processing of personal data, which includes the obtaining, recording, organising, structuring, storing, adapting, retrieving, consulting, using, disclosing, aligning, restricting, erasing, or destructing of data, whether or not by automated means.

By adhering to the principles outlined in this document, The Anthony Seddon Fund demonstrates its commitment to data protection compliance, supporting not only legal compliance but also enhancing trust and confidence in our charity and its operations.

2. Purpose

The primary purpose of this Data Protection & Confidentiality Policy is to ensure that The Anthony Seddon Fund adheres strictly to the principles of data protection as outlined by the **General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018**. This policy provides the framework for processing all personal data obtained by the charity in a manner that respects the rights of individuals and maintains their confidentiality.

Key objectives of this policy include:

- **Compliance with Legal Standards**: To ensure all data handling practices comply with statutory requirements, reducing the risk of data breaches and the potential legal repercussions associated with non-compliance.
- **Protection of Personal Data**: To protect data against loss, misuse, unauthorised access, and disclosure. This includes implementing appropriate physical, technical, and administrative measures to safeguard personal information.

- **Transparency and Accountability**: To maintain a transparent approach in our data processing activities, ensuring that stakeholders understand the methods and reasons for data collection and processing. Implementing accountability measures to demonstrate compliance with all applicable data protection rules.
- **Training and Awareness**: To provide ongoing education and training to all trustees, staff, and volunteers to ensure they understand their responsibilities under this policy and the broader regulatory framework governing data protection.
- **Support Individuals' Rights:** To support the rights of individuals regarding their personal data, such as the right to access, correct, delete, or transfer their data upon request.

3. Definitions

To ensure clarity and promote a common understanding of key terms related to data protection within The Anthony Seddon Fund, the following definitions are provided:

Personal Data
Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Processing
Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

Data Controller
The natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data Processor
A natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller.

Data Subject's Consent
Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data Protection Officer (DPO)
An expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR.

Personal Data Breach
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored, or otherwise processed.

Special Categories of Personal Data
Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; and the processing of genetic data; biometric data for the purpose of uniquely identifying a natural person; data concerning health; or data concerning a natural person's sex life or sexual orientation.

GDPR (General Data Protection Regulation)
The regulation in EU law on data protection and privacy in the European Union and the European Economic Area, which also addresses the transfer of personal data outside the EU and EEA areas.

4. Legal and Regulatory Framework

This policy operates in accordance with current data protection legislation and associated guidance governing the use of personal data in the UK. Specifically, The Anthony Seddon Fund complies with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Human Rights Act 1998 *(Article 8 – right to privacy)*
- Freedom of Information Act 2000 *(where applicable)*
- Common law duty of confidentiality

In addition to these legal obligations, The Anthony Seddon Fund also aligns with relevant best practice standards in information governance, including the ICO's Data Sharing Code of Practice, and sector-specific guidance from the Charity Commission.

Caldicott Guardian

While The Anthony Seddon Fund is not a health or social care provider and does not appoint a Caldicott Guardian, we support the ethos of the Caldicott Principles. These principles, originally developed to govern the use of personal confidential information in the NHS, promote responsible and proportionate data sharing. Their influence is reflected in our confidentiality practices, particularly where safeguarding, customer support, or partnership working is involved.

5. Responsibilities, Accountabilities and Duties

Board of Trustees

- **Oversight and Compliance**: The Board of Trustees holds ultimate responsibility for ensuring that The Anthony Seddon Fund complies with its legal obligations under GDPR and related data protection laws. The Board oversees the implementation of the Data Protection & Confidentiality Policy, reviews its effectiveness, and ensures that all necessary resources are available to support compliance.
- **Policy Approval**: Approve and endorse this policy, ensuring it reflects the strategic direction of the charity and complies with legal standards.

Data Protection Officer (DPO)

- **Compliance Monitoring**: Monitor the charity's compliance with GDPR requirements, including managing internal data protection activities, advising on data protection impact assessments, training staff, and conducting internal audits.
- **Point of Contact**: Act as the point of contact between the charity and regulatory authorities. Address all queries from data subjects and authorities related to data protection.

Chief Operating Officer

- **Policy Implementation**: Responsible for implementing the policy at an operational level, including the management of daily data handling and processing activities.
- **Incident Management**: Ensure that all data protection incidents are dealt with promptly and in accordance with legal requirements and internal procedures.

Trustees, Staff, and Volunteers

- **Compliance with Policy**: Ensure compliance with the Data Protection & Confidentiality Policy during the performance of their duties.
- **Data Handling**: Handle all personal and sensitive data in accordance with the policy and GDPR guidelines to prevent unauthorised access, disclosure, alteration, or destruction.
- **Training and Awareness**: Participate in data protection training and stay informed about best practices and legal requirements related to personal data protection.

IT Department

- **Security Implementation**: Implement and maintain adequate security measures to protect data integrity and confidentiality. This includes managing IT systems in line with data protection standards.
- **Technical Support and Incident Response**: Provide technical support to manage data securely and respond effectively to data security incidents.

Human Resources

- **Training Coordination**: Coordinate training programmes to ensure that all staff are aware of the data protection principles, their personal responsibilities, and the organisation's procedures related to personal data.
- **Documentation and Records**: Maintain records of data processing activities, training attendance, and compliance measures as required by GDPR.

All trustees, staff, and volunteers who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles. Breach of this policy may result in:

- Removal from the Board of Trustees.
- Removal from a position of employment.
- Removal from the volunteer role.
- Legal action being instigated.

6. What is Personal Confidential Data or Information?

Definition and Scope

Personal confidential data or information refers to any data that can be used to directly or indirectly identify an individual. This includes, but is not limited to:

- **Direct Identifiers**: Names, addresses, postcodes, dates of birth, NHS numbers, and other unique identifiers.
- **Indirect Identifiers**: Combinations of data that can together be used to identify a person, such as demographic information linked with contextual data.

Confidentiality and Usage

- **Protection of Data**: All information that can identify individuals must be treated as confidential. It should only be used for justifiable and legal purposes, ensuring compliance with data protection laws.
- **Anonymisation**: Wherever possible, data should be anonymised to remove any personal details that could identify an individual, thereby enhancing privacy and reducing the risk associated with data handling.

Sensitive Information

- **Special Categories**: Confidential information may include sensitive personal data as defined under data protection laws, which cover characteristics such as racial or ethnic origin, sexual orientation, health status, religious beliefs, and more.
- **Uniform Protection**: Confidential and sensitive information receives uniform protection under our policies, irrespective of the medium—digital or paper-based—in which it is stored.

Types of Information Processed

The Anthony Seddon Fund processes various types of personal information critical to its operations:

- **Employment and Volunteering**: Applications for staff and volunteer posts, including references.
- **Operational Data**: Contact details, training records of trustees, staff, and volunteers.
- **Client Data**: Customer or client information, which may include extensive case notes, is particularly relevant in service delivery settings.
- **Financial and Donor Information**: Details about funders and donors to ensure transparent and ethical financial practices.

Storage Forms

- **Digital Storage**: Personal information is stored within secure computer database systems, which are protected according to our IT security policies.
- **Physical Storage**: Paper-based files are maintained securely, accessible only to authorised personnel.

Personnel Involved in Processing

- **Roles**: Specific groups within the organisation who handle personal information include trustees, administration personnel, group facilitators, the finance team, and the peer support team, all within the scope of their designated roles and responsibilities.

7. Confidential Practices

Data Collection and Use

- **Necessity and Purpose**: Prior to collecting personal information, The Anthony Seddon Fund will assess the necessity and specificity of the information required, such as for volunteer applications or onward referrals. This ensures that only essential data is collected to fulfil defined purposes.
- **Informed Consent**: Before using personal information, trustees, staff, and volunteers must clearly communicate to groups, organisations, or individuals the purpose for which the data is collected. Explicit consent must be obtained to store and use this information, adhering to GDPR requirements.

Information Sharing and Confidentiality

- **Internal Discussions**: Trustees, staff, and volunteers may share necessary information internally to facilitate discussion and seek advice on work-related matters. Information considered sensitive, including personal, financial, or private details, must not be disclosed outside of authorised personnel without explicit consent from the individual concerned.

- **Professional Conduct**: All personnel should refrain from discussing confidential information in social settings and must avoid the informal exchange of personal details or comments that could undermine professional relationships.
- **Supervisory Consultations**: Situations requiring further insight or a different perspective should be addressed in formal debriefing or supervisory sessions, ensuring discussions are structured and confidential.

Handling External Information and Complaints

- **External Information**: If information concerning the conduct of a colleague or group is received from external sources, it should be handled sensitively. The individual providing the information should be directed to the charity's **HR-002 - Complaints Policy** for proper guidance.
- **Whistleblowing**: Staff, trustees, or volunteers holding sensitive information about potential misconduct should report their concerns through the appropriate channels as outlined in **HR-PP-CE-01 – Freedom to Speak Up & Whistleblowing Policy**. Allegations proven to be malicious or baseless will be addressed according to the charity's disciplinary procedures.

Legal Disclosure Obligations

- **Duty to Disclose**: When legally mandated to disclose information, The Anthony Seddon Fund will ensure that the affected individual is informed about the disclosure beforehand, unless doing so would compromise legal proceedings or investigations. This practice aligns with our commitment to transparency and data subject rights under GDPR.

Compliance with Policies

- **Policy Adherence**: All trustees, staff, and volunteers are required to adhere strictly to this policy and related documents. Any breaches or deviations from this policy may result in disciplinary actions and, where applicable, legal proceedings to safeguard the charity's operations and reputation.

8. Why Information is Held

The Anthony Seddon Fund collects and retains information primarily about individuals, staff, trustees, and volunteers. This information is essential for several key functions:

- **Service Delivery**: To effectively deliver services tailored to the needs of the individuals we support, it is crucial to understand their specific requirements and circumstances. Accurate and up-to-date information allows our team to provide services that are appropriately adjusted and targeted to meet these needs.
- **Performance Monitoring**: Maintaining records on the services provided enables the Fund to monitor and assess the effectiveness of our interventions. This ongoing evaluation helps ensure that our offerings

continue to meet the needs of those we serve and allows us to make necessary adjustments to enhance our impact.

- **Operational Excellence**: Information about staff, trustees, and volunteers is used to manage our internal operations effectively. This includes everything from administration, training, and development to ensuring compliance with legal and regulatory requirements. Keeping detailed records supports efficient management and operation of the Fund, facilitating seamless coordination of efforts across all levels of the organisation.

9. Access to Information

General Access Protocols

At The Anthony Seddon Fund, confidentiality and integrity of information are paramount. Information deemed confidential is strictly accessible only to trustees, staff, or volunteers who require it to deliver the highest quality of service to our clients. We adhere strictly to data protection principles to ensure sensitive information is handled appropriately.

Handling Sensitive Information

Sensitive data is accessible only to individuals directly involved in managing the specific case or service, along with their direct line managers. Such information must be marked as "confidential" and should include a list of individuals authorised to access it. This ensures that sensitive information is handled discreetly and responsibly.

Disclosure to Line Managers

Colleagues are expected not to withhold any business-related information from their Line Managers, ensuring transparency and effective supervision. Personal information unrelated to business may remain confidential to the individual.

Data Subject Access

- **Customer Records:** Customers have the right to access their personal records or information related to their organisation. Requests for access must be submitted in writing to the General Manager, providing at least 14 days' notice. Such requests must be formally signed by the individual or by a designated authority, such as the Chair, Executive Officer, or Manager in the case of organisational records.
- **Staff and Volunteer Records:** Trustees, staff, and volunteers are entitled to access their personnel records. Requests should be made in writing to the General Manager, also with 14 days' notice.

Protecting Confidentiality in Handling Documents

When working with confidential documents, care must be taken to ensure they are not visible to unauthorised individuals. This includes taking precautions when photocopying or viewing such information on computer screens to prevent inadvertent disclosure.

Subject Access Requests

Detailed protocols for handling Subject Access Requests, including how to apply, what information can be requested, and the process followed by the Fund, are detailed in Section 15 of this policy. This section provides guidance on ensuring compliance with legal obligations while respecting the rights of data subjects to access their data.

10. Storing Information

General Information Storage

- **Non-Confidential Information:** General information about organisations that does not contain sensitive data is stored in unlocked filing cabinets. These cabinets are accessible to all colleagues, ensuring that non-sensitive information is readily available for everyday business operations.

Confidential Information Storage

- **Lockable Storage:** Information pertaining to trustees, staff, volunteers, and other individuals is considered confidential and is securely stored in lockable filing cabinets. The colleague responsible for these documents must ensure that line managers are aware of access procedures to maintain operational continuity.
- **Access Controls:** Confidential personnel information for trustees, staff, and volunteers is stored under the direct oversight of line managers and is accessible only to authorised individuals such as the Chief Operating Officer and the Chairperson. Cabinets and drawers containing such information are clearly labelled 'Confidential'.
- **Emergency Access:** In cases of emergency, the Chief Operating Officer has the authority to grant access to confidential files to designated personnel to ensure the continuity of operations.

Data Security Measures

- **Document Disposal:** All confidential documentation or personal data must be securely shredded before disposal to prevent potential data breaches.
- **Digital Security:** Files containing personal information stored on computer systems must be secured with password protection to safeguard digital data from unauthorised access.
- **Off-Site Security:** The removal of information from office premises must be strictly regulated. Authorisation from the General Manager is required for transporting any personal data off-site, ensuring such data is securely managed and stored, especially when in transit. For instance, data should not be left visible in vehicles but should be locked in the boot and out of sight.

Breach Consequences

- **Unauthorised Disclosure:** Any unauthorised disclosure of personal data by trustees, staff members, or volunteers is treated as a serious breach of policy. Such incidents may lead to disciplinary action, removal from position, legal consequences, or referral to appropriate regulatory bodies, depending on the severity of the breach.

11. Duty to Disclose Information

The Anthony Seddon Fund is committed to upholding the law and ensuring the safety and wellbeing of all individuals. As part of this commitment, there are circumstances under which the charity has a legal obligation to disclose certain types of information:

- **Reporting Child Abuse**: Any suspicions or evidence of child abuse must be reported immediately to Children's Services or Social Services, as outlined in our **HR-PP-HS-23 - Safeguarding Children Policy**. This ensures that necessary protective measures are promptly initiated to safeguard the welfare of the child.
- **Illegal Activities**: Any involvement or suspicion regarding drug trafficking, money laundering, acts of terrorism, or treason must be reported to the police without delay. This is crucial for preventing harm and upholding public safety.
- **Suspicion of Crimes**: If trustees, staff, or volunteers believe that any illegal act has been committed within or outside the organisation, it is their duty to report these suspicions to the appropriate authorities. This includes any criminal actions observed during the course of their duties or within their professional interactions.
- **Risk of Harm**: Should trustees, staff, or volunteers believe that an individual is at risk of harm to themselves or others, they are required to report these concerns to the designated authority or service. This duty aims to prevent harm and ensure that appropriate support and interventions are made available.

12. Disclosures

Compliance with DBS Code of Practice

The Anthony Seddon Fund rigorously adheres to the DBS Code of Practice. This adherence ensures the correct handling, use, storage, retention, and disposal of disclosures and disclosure information. We are committed to maintaining these standards to safeguard sensitive information and ensure our compliance is beyond reproach.

DBS Checks

- **Requirement for Checks**: The Anthony Seddon Fund requires Disclosure and Barring Service (DBS) checks for all trustees, staff, and volunteers whose roles involve direct contact with vulnerable groups, including children and adults at risk. This is in line with our commitment to safeguarding the vulnerable populations we serve.
- **Informing Participants**: Before taking up their roles, all trustees, staff, and volunteers are informed about the necessity for DBS checks and the specific level of disclosure required. This ensures transparency and prepares candidates for the requirements of their prospective roles.

Management of Disclosure Information

- **Secure Storage**: All disclosure information is securely stored separate from an individual's personnel files to prevent unauthorised access. Access to this sensitive information is strictly limited to authorised personnel who require it to perform their duties.
- **Legal Restrictions on Sharing**: It is a criminal offence to share disclosure information with individuals who are not legally entitled to receive it. The Anthony Seddon Fund enforces strict controls to prevent such unauthorised sharing, ensuring compliance with legal obligations.
- **Record Keeping**: The Fund meticulously records each disclosure, documenting the date of issue, the subject's name, the type of disclosure requested, the position it pertains to, the disclosure's unique reference number, and the recruitment decision taken. This detailed record-keeping supports transparency and allows for effective monitoring of compliance and decisions related to staffing.

13. Breach of Confidentiality

Addressing Internal Concerns

- **Proper Channels for Complaints**: Colleagues who have concerns or are dissatisfied with the conduct or actions of their peers are strongly encouraged to address these issues through the proper channels. This includes speaking directly with their Line Manager or a trustee. It is vital to maintain professionalism and confidentiality by refraining from discussing these concerns outside The Anthony Seddon Fund to safeguard the privacy and reputations of all involved.

Consequences of Breaching Confidentiality

- **Unauthorised Access and Disclosure**: Trustees, staff, and volunteers, whether current or former, must not access or disclose confidential information without proper authorization. Engaging in such activities is considered a serious breach of trust and confidentiality.
- **Legal and Disciplinary Actions**: Individuals found to have unauthorised access to confidential files or who breach confidentiality will face disciplinary

actions, which may include termination of employment or volunteer status. Additionally, legal action may be pursued if the breach involves severe misconduct or results in significant harm or risk to individuals or The Anthony Seddon Fund.

14. Whistleblowing

Policy Compliance

- **Scope and Obligation**: Trustees, staff, and volunteers are obliged to report any concerns related to the misuse of the charity's data or information or any improper practices by individuals within the organization. This responsibility extends to all forms of misconduct, whether they pertain to data handling, breaches of confidentiality, or other ethical violations.
- **Guidance and Procedure**: All reports should be made in accordance with the guidelines set out in **HR-PP-CE-01 – Freedom to Speak Up & Whistleblowing Policy**. This policy provides a structured approach for raising concerns, ensuring that they are handled sensitively, confidentially, and effectively.

Encouragement of Transparency

- **Supportive Environment**: The Anthony Seddon Fund is committed to maintaining an environment where open communication is encouraged and protected. We ensure that all personnel feel supported and secure when raising genuine concerns, without fear of retaliation or disadvantage.

Action and Resolution

- **Investigation and Response**: Upon receiving a report, appropriate steps will be taken to investigate the matter thoroughly. Corrective actions will be implemented as needed to address any substantiated issues. The process and outcomes are managed transparently, with respect to confidentiality, and in line with legal and ethical standards.

15.Training & Awareness

Comprehensive Training Programme

- **Policy Education**: All trustees, staff, and volunteers will receive thorough training on the Data Protection and Confidentiality Policy. This ensures everyone is aware of the policy details, how they apply to various roles, and the importance of adhering to these standards to protect personal and sensitive information.
- **Caldicott Principles**: Specific briefings on the Caldicott Principles will be provided, particularly for roles that handle or have access to patient or client information. These principles are crucial for understanding how to manage

healthcare-related information in a way that respects patient confidentiality and privacy.

- **Roles and Responsibilities**: Training sessions will clarify the specific data protection responsibilities associated with different roles within the organisation. This aims to ensure that all personnel are aware of their duties in terms of handling information securely and ethically.
- **Mandatory Information Governance Training**: Annual Information Governance training is mandatory for all staff to reinforce their knowledge and update them on any changes in data protection legislation or organisational policies.

Targeted Training for Specific Roles

- **Specialised Training**: Additional, role-specific training will be provided for staff members who have particular responsibilities in information governance. This training will be tailored to address the unique needs and challenges associated with their duties, enhancing their skills in managing information securely and in compliance with legal standards.

16. Subject Access Requests

Rights of Data Subjects

The Anthony Seddon Fund is committed to upholding the rights of individuals whose personal information it processes. Data subjects have the right to:

- **Access**: Understand precisely what information the charity holds about them and how it is processed.
- **Update Information**: Request updates or corrections to their information to ensure accuracy.
- **Compliance Transparency**: Receive clear information about the charity's actions to comply with data protection laws.
- **Restrict Processing**: In certain circumstances, individuals may request that the processing of their personal data be restricted.
- **Rectification and Erasure**: Request the correction or deletion of incorrect or outdated information.

Procedure for Making a Subject Access Request

- **Submitting Requests**: Requests for access to personal data must be made in writing to:

General Manager
The Anthony Seddon Fund
12 George Street
Ashton-under-Lyne
OL6 6AQ

- **Required Details**: The request should include the reason for the request, specific details about the information required, and the timeframe for the request.
- **Verification of Identity**: To protect the confidentiality of information, proof of identity is required from the requester. Acceptable forms of ID include a passport, driving license, or birth certificate.

Response Time

- **Handling Requests**: The charity strives to respond to all access requests swiftly and courteously. We aim to fulfil these requests within 30 days of receipt, as mandated by data protection legislation.
- **Additional Information**: For detailed guidance on how records can be accessed, refer to **HR-PP-IG-04 - Access to Records Policy**.

17.Review

This policy will be reviewed in line with The Anthony Seddon Fund's policy review cycle, which operates on a tiered system based on risk, relevance, and compliance need:

- **Tier 1** – Annual review (compliance-critical policies)
- **Tier 2** – Review every two years (operational or people-focused policies)
- **Tier 3** – Review every three years (low-risk or informational policies)

In addition to the scheduled cycle, this policy may also be reviewed earlier if:

- There are significant changes in legislation or best practice.
- Internal monitoring, feedback, or incidents indicate a review is necessary.
- Structural or operational changes within the charity affect its relevance or application.

Whether or not there were substantive changes, the version control section will display the date of the most recent review.