Confidentiality Policy for Face-to-Face Interactions with AKU Patients

May 2026

1. Introduction

This Confidentiality Policy outlines the commitment of AKU Society to protect the privacy of patients with Alkaptonuria (AKU) during all face-to-face interactions. Its purpose is to ensure that personal and health information shared by AKU patients in consultations, examinations, support sessions, or any in-person meetings is kept confidential and used appropriately. The scope of this policy extends to all employees, volunteers, and contractors who interact with AKU patients, and covers all forms of patient information (oral communications, written records, and electronic data) obtained in these face-to-face settings.

Maintaining confidentiality is essential for fostering trust between patients and those caring for them. Patients have a right to expect that their personal health details and personal conversations shared will remain private and protected. This policy is founded on that principle and ensures that every staff member understands and upholds the duties of confidentiality when dealing with AKU patients.

2. Legal and Ethical Compliance

- **Compliance with Laws**:

AKU Society complies with all relevant data privacy laws and healthcare regulations to protect patient information. This includes adherence to the EU[HD1] General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018, which set strict requirements for processing personal data. We also operate under the common law duty of confidentiality and respect patients' rights to privacy as defined in laws such as the Human Rights Act 1998. All employees and representatives are bound by a legal duty of confidence regarding any personal information they encounter in the course of their work. Violating patient confidentiality is not only an ethical breach but can also violate these laws, potentially leading to legal consequences for the individual and the organisation.

- **Ethical Standards:**

In addition to legal obligations, our staff must follow the professional ethical standards relevant to their roles. Healthcare providers (doctors, nurses, and allied professionals) are expected to abide by their regulatory bodies' guidelines on patient confidentiality (for example, the GMC's Confidentiality guidance for doctors, the NMC Code for nurses, etc.). All staff and volunteers are trained to understand that respecting patient privacy is a core ethical duty. We integrate key principles from ethical codes and national guidelines (such as the NHS Confidentiality Code of Practice and the Caldicott Principles) into our daily practices to ensure that handling of AKU patient information meets the highest standard of integrity. By complying with both the law and professional ethics, we aim to protect patient dignity and confidentiality at all times.

3. Confidentiality Principles

All personnel are expected to follow these foundational principles of confidentiality when engaging in face-to-face interactions with AKU patients and handling their information:

- **Minimum necessary use:**

Collect, use, and disclose only the minimum amount of patient information required to perform your duties or achieve the specific purpose. Unnecessary or unrelated details should not be requested or recorded. This principle ensures that we do not intrude on a patient's privacy more than is absolutely needed for their care or support.

- **Need-to-know access:**

Access to patient information is strictly on a need-to-know basis. Only authorised staff who are directly involved in a patient's care or administration should view or hear their personal details. If you do not need certain information to fulfil your role, you should not seek it out. Even within the healthcare team, team members should only share the specific details relevant to each other's responsibilities.

- **Private communication:**

Ensure conversations with or about patients occur in private settings to prevent unauthorised people from overhearing. During face-to-face consultations or discussions, speak discreetly and avoid discussing patient cases in public areas, where possible (hallways, elevators, cafeterias, etc.). If others are nearby, take reasonable steps (lowering voices or moving to a confidential space) to maintain privacy. We do not discuss patient information with anyone outside the care context, and certainly not in any forum where it might be overheard by those who have no right to that information.

- **Security of information**:

Treat all patient records and notes as confidential and handle them securely at all times. Do not leave documents, forms, or electronic devices that contain patient information unattended or visible to unauthorised individuals. For example, avoid placing patient files in open view in clinic areas accessible to other patients, and always log out of computer systems when finished, to prevent inadvertent disclosure. (Specific data security measures are detailed in Section 4 below.)

- **Transparency and respect:**

Be honest and transparent with patients about how their information will be used. If an AKU patient asks about our confidentiality practices, staff should be able to explain that their data is protected and only shared in the ways this policy outlines. Also, respect any patient preferences or concerns regarding privacy—if a patient requests extra discretion in how their information is handled or shared, we will accommodate this wherever possible within legal and care requirements.

These principles are in line with widely accepted standards in healthcare confidentiality. They reflect the Caldicott Principles used in the UK: for instance, using only necessary information, sharing on a need-to-know basis, and ensuring everyone understands their responsibility to protect confidentiality. By following these guidelines, we maintain a high level of privacy and trust in all face-to-face interactions with AKU patients.

4. Data Collection and Storage

- **Data Collection:**

We only collect personal and health information from AKU patients that is relevant and necessary for their care, treatment, or the services we provide. During face-to-face encounters, staff will explain why particular information is being requested (for example, explaining that we ask about symptoms or family history to inform treatment plans). Patients are not required to divulge information unrelated to their healthcare or support. If a patient chooses not to share certain details, we will respect their decision, though staff will inform them if this might limit our ability to provide comprehensive care or services.

- **Secure Handling:**

All patient data obtained through in-person interactions (such as medical histories, consultation notes, test results, or personal contact details) is handled with strict security. Physical records (paper files, forms, handwritten notes) are kept in locked cabinets or secure file rooms accessible only to authorised personnel. Electronic records (entries in databases, digital documents, emails, etc.) are protected by passwords, user authentication, encryption, and other IT security measures. We implement appropriate technical and organisational safeguards to protect personal data against unauthorised access, alteration, loss, or damage. For example, only staff with the proper clearance can access electronic health records, and all access is logged and monitored. Portable devices containing patient information (like laptops or tablets used in clinics) are encrypted and should never be left unattended in public places.

- **Storage and retention:**

AKU Society adheres to the data storage limitation principle under GDPR, which means we do not keep patient information longer than necessary. Personal information is retained only for the period required to fulfil the purposes for which it was collected (such as ongoing medical care or as required by law). We follow any applicable healthcare record retention guidelines; for instance, health records may be kept for a minimum number of years as mandated by national policy or regulatory bodies. Once the retention period is met, or if the information is no longer needed, we dispose of the data in a secure manner. Paper records are shredded or incinerated, and electronic data is permanently deleted or anonymised, in a way that ensures it cannot be reconstructed. Should a patient cease to receive services from us, their records will be archived or destroyed in compliance with legal requirements and our retention schedule. Throughout the storage period, we continuously maintain the confidentiality and security of the data.

By limiting data collection to what is necessary and safeguarding stored data, we comply with GDPR's fundamental principles of data minimisation, integrity, and confidentiality. Our goal is to ensure that at every stage—collection, storage, use, and eventual disposal—AKU patient information remains private and protected from unauthorised access or disclosure.

5. Information Sharing and Disclosure

We treat all information shared by AKU patients as confidential and do not disclose it to others unless certain conditions are met. Below are the guidelines on how and when patient information may be shared or disclosed, consistent with patient consent, legal requirements, and medical necessity:

• **Within the healthcare team (care continuity):**
Members of the patient's healthcare team may share relevant information with each other for the purpose of providing care to the patient. This is considered a "medical necessity" or implied consent situation – patients generally understand that doctors, nurses, specialists, and other healthcare professionals involved in their treatment will communicate as needed about their condition. Such sharing is done on a need-to-know basis and limited to what each team member needs to know to do their job effectively. For example, a specialist may share a summary of findings with the patient's GP, or a nurse may update a consultant on the patient's symptoms. This kind of information exchange is vital for safe, coordinated care and is supported by ethical guidelines. All staff will continue to handle the information discreetly and ensure it's not accessible to anyone outside the care team.

• **Patient consent for external disclosures:**
Outside of the immediate care team, we will not share a patient's personal information with any third party unless we have the patient's explicit consent, except in the special circumstances noted below. This means that if an AKU patient wants us to share information with a family member, caregiver, social services, an employer, or any other person/organisation, we will do so only if the patient has given clear permission. Wherever possible, this consent should be documented (for instance, by having the patient fill out a consent form specifying what information can be shared and with whom). Patients can also specify any limits on the information to be disclosed. For example, a patient might consent to us discussing general health updates with a relative but not specific test results. If the patient is under 18 or otherwise unable to give informed consent, we will follow applicable laws regarding who can consent on their behalf (e.g., parental responsibility or power of attorney). In all cases, the patient's wishes guide our disclosure – if they do not want certain information shared, we will honour that choice unless overridden by a legal obligation or serious safety concern (as described below).

• **Legal and ethical exceptions (permitted disclosures without consent):**
In rare cases, we may be required or permitted by law to disclose patient information without their consent. Such exceptions to confidentiality are taken very seriously and occur only under specific conditions, such as:

• **Serious threats or harm prevention:** If a patient reveals information indicating that they pose an imminent serious threat to themselves or others, or if there is a concern of serious harm (for instance, risk of suicide, threat of violence, or suspected abuse of a vulnerable person), staff may have a professional duty to breach confidentiality to prevent harm. In such cases, information would be shared only with the appropriate persons or authorities who can help mitigate the risk (for example, alerting mental health crisis teams or the police). Similarly, if we suspect child abuse or abuse of an at-risk adult, we are often legally obligated to report it to social services or safeguarding authorities. These situations are guided by "duty to warn" or mandatory reporting laws – while confidentiality is crucial, it may be ethically justified to override it if doing so will protect someone from serious harm.

• **Public health and safety**: During public health emergencies or to control communicable diseases , health authorities may require certain patient data (like diagnosis of a notifiable disease) to be reported for the greater public good. In these instances, we will provide the required information to the proper public health agency as the law demands. Additionally, if not sharing the information would likely result in a crime being committed or pose a grave risk to the community, we will weigh the situation in consultation with legal/ethical advisors and may disclose to the proper authorities as necessary.

In all the above scenarios, any disclosure without consent will be limited to the minimum information necessary and shared only with those who need to know it. The incident will be documented, including the reason for disclosure and to whom the information was given. We will also inform the patient about the disclosure, unless doing so would further jeopardise safety (for example, in some abuse reporting cases we may be advised not to inform the perpetrator). These exceptions are in place to comply with laws and ethical obligations, but they are applied with great care and only when absolutely warranted.

- **Restricted access for others:**

Aside from the care team and the specific exceptions above, no one else is allowed access to a patient's confidential information. We do not divulge patient details to friends, other patients, media, or any unauthorised individuals. Even confirming whether someone is a patient of AKU Society is considered confidential. For example, if an inquiry is made asking, "Is John Doe an AKU patient at your clinic?", our staff will neither confirm nor deny this without patient consent, because simply acknowledging someone as a patient can breach their privacy. This policy holds even if the person asking is well-intentioned or already claims to know details (such as a family member who was not explicitly authorised by the patient). Staff are trained to politely refuse or redirect such queries, explaining that they cannot release any information due to confidentiality.

• **Use of data for training or research:**

If patient information is to be used for purposes beyond direct care – for instance, in medical research, case studies, or training materials – we will either fully anonymise the data (remove all personally identifying details) or obtain the patient's explicit consent. Any identifiable patient information will not be published or shared externally (in conferences, journals, etc.) without consent. This ensures that patients retain control over whether their personal story or medical data is used in broader contexts.

In summary, we will not share AKU patient information with anyone outside the immediate care context unless the patient agrees. When sharing is necessary (either for care or due to an overriding legal imperative), we do so carefully, sharing only what is required, and we document the exchange. By following these guidelines, we uphold both the patient's privacy and the communication needed for safe treatment, in line with GDPR's requirements for lawful processing and the fundamental ethical duty of confidentiality.

6. Staff Responsibilities

All members of staff, as well as volunteers and any trainees or contractors who interact with AKU patients, have critical roles in maintaining confidentiality. Each individual is personally responsible for safeguarding patient information. The following obligations apply to all staff:

• **Adherence to policy:**

Staff must read, understand, and comply with this Confidentiality Policy and all related procedures. This is a condition of employment or engagement. Upon joining AKU Society[HD1] , every staff member signs a confidentiality or non-disclosure agreement affirming their commitment to protect patient information. By signing, they acknowledge that they understand their duty to keep patient data private and the consequences of failing to do so.

•**Access on a need-to-know basis:**

Staff should only access patient information that they need to know to perform their specific job functions. For example, a physician will access medical records to treat the patient, whereas an administrative assistant may only need contact details for scheduling. No staff member should ever look at a patient's records or listen to patient conversations out of curiosity or without a work-related purpose. Browsing through records of friends, family, neighbours, or well-known individuals out of personal interest is strictly forbidden and is a breach of confidentiality. Our systems and procedures are designed to support this principle (with access controls in electronic records, etc.), but it is ultimately each staff member's responsibility to follow through and respect these boundaries.

- **Secure handling of information:**

Staff must handle all patient-identifiable information with care and security. This means keeping documents and files secure at all times – do not leave confidential documents unattended or in public areas. For instance, if you have paper notes from an AKU patient consultation, ensure they are filed properly or kept with you until they can be secured; never leave them on a desk in a shared office where unauthorised people could see them. Similarly, computer terminals should be logged off or locked when not in use. Staff should not share their login credentials or allow others to access systems under their account. Conversations about patients should be conducted privately (as discussed in section 3); staff must refrain from discussing patient cases in corridors, cafeterias, or outside of work. Even at home or off-duty, staff should not share stories or details about identifiable patients. The obligation to confidentiality extends beyond the workplace and continues even after a staff member's employment ends.

• **Reporting and escalation:**

If a staff member becomes aware that confidentiality may have been breached (for example, they realise they sent an email to the wrong recipient, or they witness someone accessing records improperly), they have a responsibility to report it immediately (as outlined in Section 8 on breach management). Staff should also feel empowered to speak up if they notice practices that could lead to breaches (such as files left out, or someone without authorisation attempting to get information). Additionally, if any staff member is unsure about whether certain information can be shared or how to handle a particular situation, they must seek guidance from from our CEO or Head of Patient Support & Welfare before taking action. It is always better to ask and clarify than to risk an improper disclosure.

Disciplinary consequences: Upholding patient confidentiality is a fundamental job requirement. Any breach of this policy or misuse of patient information by staff is taken extremely seriously by AKU Society. Violations can lead to disciplinary action, up to and including termination of employment or contract, in accordance with our HR policies and applicable laws. For instance, deliberately accessing or sharing confidential data without authorisation, or gross negligence in handling information (such as leaving a patient file in a public place), can be considered gross misconduct. In some cases, particularly egregious breaches may also carry legal penalties for the individual (under data protection laws or professional regulatory rules). We want to emphasise that maintaining confidentiality is not just about avoiding punishment – it's about preserving the trust that patients place in us. All staff are reminded regularly of these responsibilities and the serious nature of confidentiality breaches. By being diligent and conscientious, staff contribute to a safe environment where AKU patients can feel confident that their personal information remains private.

7. Patient rights

AKU patients have several rights regarding their personal data and how it is handled by AKU Society. We are committed to upholding these rights, in compliance with GDPR and healthcare privacy regulations, and to empowering patients with control over their own information. Key patient rights include:

• **Right to be informed:**

Patients have the right to be informed about how their personal information is collected, used, stored, and shared. We fulfil this by providing clear privacy notices and explanations.

At the start of care (for example, during an intake appointment or registration), we inform patients about our confidentiality practices and data usage. Patients will be told what information we collect and why, who it may be shared with, how long we retain it, and the safeguards in place. This transparency allows patients to understand what will happen with their data and is a fundamental principle under GDPR (the right to be informed).

- **Right of access:**

Patients have the legal right to access the personal health information that we hold about them. This is often referred to as a Subject Access Request under GDPR. An AKU patient (or an authorised representative) can request a copy of their medical records or any other personal data we have in our files. In response, AKU Society will provide the information in an accessible format, usually within one month as required by law. This includes records of face-to-face consultations, test results, care plans, and any correspondence. We will verify the identity of the requestor to ensure we don't release data to the wrong person. Patients will generally not be charged a fee for accessing their data (unless a request is repetitive or excessive, in which case a reasonable fee may be permitted by law, though this is rare). By facilitating access, we enable patients to stay informed about their own health information and correct any inaccuracies.

- **Right to rectification (correction):**

If a patient believes that any personal information we hold about them is incorrect or incomplete, they have the right to request that we correct it. We encourage patients to review the information we have (for instance, check that their contact details are up to date, or that clinic notes accurately reflect what they said). Should an error be found – e.g., an incorrect date of birth, a misspelled name, or a misrecorded symptom – AKU Society will rectify it promptly and inform the patient once the correction is made. If the accuracy of certain data is disputed (for example, a patient disagrees with a diagnosis or a professional opinion in the record), we may not erase the original note (since it may have been an accurate record of the opinion at that time), but we will add the patient's statement or clarification to the file so that their perspective is also documented. Patients can make rectification requests verbally or in writing, and we will respond within one month as mandated by GDPR. Ensuring data accuracy is important not only for patient trust but for effective healthcare, so we take these requests seriously.

- **Right to object, restrict processing, or request erasure:**

Patients have rights to control certain uses of their data beyond just viewing or correcting it. They may object to specific types of data processing or ask us to restrict processing. For example, an AKU patient might object to us using their data for a research registry or for marketing of a hospital service. They might request that we "freeze" use of their data in some way – this could occur if they contest the accuracy of the data (asking us not to use it until it's fixed) or if they simply want to limit how we use their information. AKU Society will consider and comply with such requests when possible, as long as it does not conflict with our legal obligations or the provision of essential medical care. Additionally, patients have the right to request erasure of their data ("right to be forgotten") in certain circumstances – for instance, if the data is no longer needed, or if it was processed based on consent which they now withdraw. However, it is important to note that the right to erasure is typically limited in a healthcare context. Health providers are often required by law to retain medical records for a minimum period (for continuity of care, legal defence, public interest, etc.), so we cannot usually honour requests to delete medical records immediately. In fact, UK regulations and NHS guidelines mandate retention of health records for set time frames, making deletion requests uncommon to grant. That said, if a patient has compelling reasons for wanting some personal data removed and it's information not needed for ongoing treatment or legal purposes, our team will review the request. Where we cannot fully erase data due to legal requirements, we will inform the patient of the reason. We might instead offer to restrict the data from routine use. All decisions on objections, restrictions, or erasure requests will be communicated to the patient, and we will do our best to accommodate their preferences while balancing regulatory responsibilities.

Right to withdraw consent:

In cases where the patient's consent is the basis for processing their data (for example, if a patient consented to share information with a research project or to allow use of their photograph in an AKU awareness campaign), they have the right to withdraw that consent at any time. We make it as easy as possible for patients to change their mind. If consent is

withdrawn, we will stop the particular use of data that was based on consent. (Note: For most core healthcare activities, we rely on legal bases other than consent – such as providing medical care – so withdrawal of consent typically applies to optional data uses.) Withdrawing consent will not affect any data processing that has already occurred, but it will prevent future use of the patient's data in that manner. There is no penalty or impact on medical care if a patient chooses not to consent or to withdraw consent for a non-essential use of their data.

- **Right to complain and seek redress:**

We prioritise patient satisfaction and encourage patients to voice any concerns about their privacy or our data handling practices. If an AKU patient believes their confidentiality has been breached, or that their data protection rights have not been respected, they have the right to complain. Patients are urged to contact AKU Society first – for instance, they can reach out to our team to report their concern. We will treat such complaints seriously, investigate thoroughly, and respond with the outcome and any actions we will take to resolve the issue. We have a formal complaint procedure to ensure fairness and timeliness in this process, and patients will be given information on how to use it (e.g., a brochure or website outlining the steps). If a patient is not satisfied with our response or if they prefer, they also have the right to escalate their complaint to the relevant supervisory authority. In the UK, this is the Information Commissioner's Office (ICO), which oversees data protection compliance. Patients can contact the ICO to report a confidentiality/data protection concern or to seek assistance in resolving the matter. In fact, patients have the right to apply to the ICO to make a complaint or to have their health records reviewed for accuracy and lawfulness. The ICO has the power to investigate and can order organisations to correct issues or improve practices. Similarly, if appropriate, patients could bring concerns to other bodies like professional regulators (for example, if they felt a doctor mishandled information, they could inform the GMC). We will cooperate fully with any external investigation and work to put things right. Importantly, raising a complaint or exercising any of these rights will never negatively affect the care an AKU patient receives; we strictly prohibit any form of retaliation or reduced service due to a patient asserting their rights.

To summarise, we recognise that patients are the owners of their personal information and have rights to control and know about its use. AKU Society has procedures in place to uphold each of these rights. We also make sure to inform AKU patients of these rights in a user-friendly way (through notices or conversations) so that they can confidently engage with us on privacy matters. By honouring patient rights, we not only comply with GDPR and healthcare laws, but we also build trust with the AKU community we serve.

8. Breach Management

Despite rigorous precautions, there is always a possibility (however small) of a confidentiality breach or data security incident. A "breach" could include any unauthorised access, disclosure, loss, or alteration of patient information – for example, a lost file, a misdirected email containing patient data, an improper conversation heard by others, or any situation where confidentiality is compromised. AKU Society has a clear procedure for handling such incidents to ensure they are addressed promptly and transparently. The following steps outline our breach management process:

1. Immediate reporting:

All staff must report any actual or suspected breach of confidentiality immediately. If an employee or volunteer becomes aware of a potential breach (e.g., realises they sent a patient's test results to the wrong person, finds a patient document missing, or witnesses someone viewing records improperly), they are required to notify the CEO or Head of Patient Support & Welfare without delay. The key is speed, the sooner we know about an issue, the faster we can act to contain it. Staff should not try to cover up or ignore a breach; our culture is one of transparency and blame-free reporting. There will be no retaliation for reporting a concern – in fact, failure to report a known breach could result in disciplinary action. Once a report is made, the organisation will log the incident in our incident tracking system.

2.. Containment and investigation:

Upon notification, our first priority is to contain the breach to prevent further compromise. This might involve actions like isolating or shutting down a compromised IT system, recovering mis-sent or lost documents if possible, asking the unintended recipient of information to delete or return it, or securing any physical area involved. We then launch an investigation to ascertain the details of the breach. The CEO or Head of Patient Support & Welfare will determine the scope of the breach (what information and which patients are affected, how many individuals are impacted), the cause (e.g., human error, technical failure, malicious action), and the potential consequences for the patients (any risk of identity theft, embarrassment, harm to care, etc.). The team will gather all relevant facts by interviewing staff involved, reviewing system logs, and so forth. Our goal is to understand exactly what happened and what risks result. During this phase, we also ensure that any immediate corrective actions are taken – for example, if a security weakness is identified (such as a software flaw or an insecure process), we will fix or halt use of that system to prevent additional incidents.

3. Notification and communication:

Once we have initial facts and have contained the incident, we assess whether the breach triggers any notification requirements. Under GDPR, if a personal data breach is likely to result in a risk to individuals' rights and freedoms, we must notify the supervisory authority (ICO) within 72 hours of becoming aware of the breach. If the breach is likely to result in a high risk to the affected individuals (for example, it involves sensitive health details that have been exposed), we also will inform the patients concerned without undue delay, in clear language about what happened and any steps they should take to protect themselves. AKU Society will comply with these legal obligations. Our CEO or Head of Patient Support & Welfare will make a case-by-case decision, following ICO guidelines, on whether external notification is needed. Even if a breach doesn't legally require reporting, we may still choose to inform patients if we believe it is the right thing to do for transparency. When notifying patients about a breach, we will explain what data was involved, what we are doing about it, and offer support (for instance, guidance on monitoring their accounts if financial info was involved, or simply an apology and point of contact for questions). We also communicate internally – relevant managers and executives will be informed of the incident status. Throughout the process, we maintain documentation of all decisions regarding notifications.

4. Remediation and follow-up:

After the immediate response, AKU Society takes steps to address the root cause of the breach and prevent similar incidents in the future. All breaches and near-misses are analysed to identify lessons learned. Depending on the findings, we might update our procedures, improve security controls, or provide additional training to staff. For example, if a breach occurred because a staff member didn't follow protocol, we might reinforce training or revise that protocol for clarity. If it was due to a technical issue, we will work with our IT department to patch or upgrade systems. Every breach is logged and reviewed by management. The outcome of the investigation, including what happened and what has been done to fix it, is recorded in an incident report. Where individual staff are found to have violated policy deliberately or through gross negligence, appropriate disciplinary action will follow, consistent with HR policies (this could range from additional training and supervision up to termination in severe cases). Our goal is not only to correct the specific incident but to strengthen our overall confidentiality practices. Additionally, we will consider if the breach should be communicated in aggregate form to the AKU patient community (for example, as part of a transparency report) – but we will never publicly reveal identities or specifics unnecessarily. Finally, we ensure that any promises made to patients or regulators (such as providing follow-up information or support) are fulfilled.

By following this structured approach to breach management, we aim to mitigate any damage quickly and preserve patient trust even in the event of a mistake or accident. We recognise that how we handle a breach is a reflection of our commitment to confidentiality. Thus, we respond swiftly, communicate honestly, and take concrete steps to prevent recurrence. Patients can be assured that, should an incident occur, we will do everything in our power to right the situation and protect their interests.

9. Training and Compliance Monitoring:

Staff training:

Ensuring that all team members understand confidentiality is a top priority. AKU Society provides comprehensive training on data protection and patient privacy to all staff and volunteers upon onboarding, and at regular intervals thereafter. New employees attend an induction session which includes sessions on confidentiality, GDPR, and our specific policies and procedures for handling patient information. In addition to initial training, we conduct refresher training sessions periodically (typically annually, or more frequently if needed) to keep everyone updated on any changes in laws or policies. We also provide targeted refresher courses if we observe particular issues — for instance, if a trend of minor breaches is noted, we might organise a focused workshop on that topic. Training materials are available for reference (such as employee handbooks), and we encourage staff to review them whenever in doubt. By investing in regular education, we foster a culture where confidentiality is understood, valued, and practiced consistently.

Ongoing awareness:

Beyond formal training, we keep confidentiality in the forefront of staff consciousness through various means. All staff are required to acknowledge the confidentiality policy (for example, signing off that they've read updates) whenever it's revised. Through continuous learning and reminders, we aim to ensure that protecting patient privacy becomes second nature in daily routines.

Accountability:

Leadership is accountable for enforcing this policy. CEO or Head of Patient Support & Welfare must ensure their teams are trained and adhering to protocols. We may also include confidentiality compliance as part of employee performance evaluations in roles where it is especially critical. Staff are expected to cooperate fully with any compliance checks or investigations. Where lapses are identified, we take corrective action promptly – this could be as simple as coaching a staff member, or as formal as updating a policy. We document these monitoring activities and outcomes as part of our commitment to accountability.

Overall, through systematic training and monitoring, we create a robust environment where staff are knowledgeable about confidentiality and consistently follow best practices. We strive to catch and correct any issues early, before they lead to breaches. Our patients trust us with sensitive information; through ongoing education and vigilance, we ensure that this trust is well placed and maintained.

10. Review and Updates

This Confidentiality Policy is a living document and will not remain static. We conduct periodic reviews of the policy to keep it up-to-date with evolving laws, regulations, and best practices. At a minimum, the policy will be formally reviewed on an annual basis to ensure it remains current and effective . During each review, we will assess whether any changes in relevant legislation (such as updates to GDPR or healthcare regulations) or changes in our operational practices necessitate revisions to the policy. For instance, if new guidance is issued on patient data protection or if AKU Society adopts a new system for record-keeping, we will update the policy accordingly.

Reviews may happen more frequently than annually if needed. Trigger events for an out-of-cycle review could include: significant changes in data protection law, the occurrence of a serious confidentiality breach (which might highlight gaps in the policy), the introduction of new technology for handling patient information, or feedback from patients and staff that suggests clarifications are needed.

Update procedure: When an update is made, the revised policy will be approved by the appropriate authority within the organisation (e.g., CEO or Head of Patient Support & Welfare). We will version-control our policies, so the document will note the date of the latest revision and a summary of changes if applicable. After approval, AKU Society will communicate changes to all staff and volunteers. This could be done via official memos, email announcements, and re-training sessions if the changes are substantial. We will also make the updated policy available to patients upon request and might post it on our website or in our facilities for transparency.

All staff are expected to stay informed of the current policy. Compliance with the updated policy will be monitored as described in Section 9. If any amendments significantly affect how we handle patient information, we will incorporate those into staff training and patient communication as necessary.
By regularly reviewing and updating this policy, we ensure that it remains aligned with the latest legal requirements (such as GDPR), incorporates emerging best practices in patient privacy, and addresses any practical issues encountered in our face-to-face work with AKU patients. This continuous improvement approach allows AKU Society to maintain the highest standards of confidentiality. The trust that AKU patients place in us is paramount, and keeping our confidentiality policy rigorous and up-to-date is one of the ways we honour that trust.

Next Review Due: May 2027

Effective date: 11/5/2026

Signature: