2025
EDITION

ANGLICAN CHURCH OF KENYA

DATA PROTECTION POLICY

Contents

Welcome

Embracing Our Shared Responsibility in Data Protection

It is my privilege to introduce this Data Protection Policy, a cornerstone in our collective journey toward safeguarding personal and sensitive information entrusted to us. This policy symbolizes our shared responsibility to uphold privacy, ethical responsibility, and the stewardship of data in all our ministries and services.

In this era of digital transformation, where information flows faster and wider than ever before, ACK stands resolute in its commitment to ensuring the protection of all data we manage. This is in recognition that personal information is not merely data but a reflection of the dignity and worth of individuals, we approach this endeavour with profound respect and accountability.

This policy is constructed to provide practical and actionable guidelines tailored to the diverse contexts in which ACK operates. Its intent is not only to comply with the legal requirements set forth by the Constitution of Kenya and the Data Protection Act of 2019 but also to embrace global standards, as an extension of our Christian values. We emphasize the importance of safeguarding sensitive information, including the data of children, as a testament to our commitment to compassion and care.

To the clergy, staff, volunteers, and stakeholders who will engage with this policy, I extend my heartfelt thanks and encouragement. Let this document be a tool to strengthen trust within our community and an inspiration that guides us to embody the principles of justice, confidentiality, and ethical management of information. It is through these shared efforts that we can reflect the love and wisdom of Christ in every aspect of our stewardship.

Together, we can set a precedent—one that integrates faith with responsibility, and values with action. May this policy enrich our mission and empower us to serve with integrity, compassion, and unwavering commitment.

Kind regards

Rt. Rev. Prof. Joseph Galgalo
Provincial Secretary
(*Nairobi, 2025*)

Forward

I am honoured to write a foreword to this ACK Data Protection Policy. In an age defined by technological advancements and the complexities of digital information, we acknowledge the sacred trust entrusted to us in handling personal data. This policy is not just a legal obligation but a reflection of our theological commitment to dignity, respect, and stewardship.

Rooted in our belief that every individual is created in the image of God, this policy underscores the importance of safeguarding personal information as a matter of justice and love. The Constitution of Kenya, alongside the Data Protection Act of 2019, provides the legal framework within which we operate, ensuring that we meet both national and international standards in managing sensitive data. Inspired by global norms such as the EU's GDPR and the United Nations Guidelines on Data Protection, we have adopted principles that embody fairness, transparency, integrity, and accountability.

This policy is structured to be a guiding light for all ACK entities—from dioceses and parishes to schools, hospitals, and developmental services. It is designed to be practical, addressing the complexities of data collection, storage, and use while safeguarding the rights and dignity of the individuals whose information we handle. It emphasizes our commitment to confidentiality, secure data practices, and the special care required in managing sensitive information, such as children's data.

In implementing this policy, ACK aims to foster trust within our community, reflecting our Christian ethos in every aspect of data stewardship. It is our hope that this policy will not only fulfill our legal obligations but also strengthen the bonds of love and respect among clergy, congregants, staff, students, and all stakeholders.

May this policy serve as a testament to our dedication to justice, integrity, and the responsible use of knowledge, as we seek to honour God through our work and ministry. Let it be a source of guidance and inspiration for all who engage with it.

Yours in Christ's service,

The Most Rev. Dr. Jackson Ole Sapit
Archbishop
(*Nairobi, 2025*)

Policy Approval Statement

This Data Protection Policy for the Anglican Church of Kenya (ACK) was officially adopted by the Provincial Synod of ACK and comes into effect upon the date of approval. The Policy has been duly reviewed and endorsed through the Church's governance processes, reflecting our collective commitment to protect personal data in all our ministries.

Approval: This document was presented to the Provincial Synod in Session and approved on [**Date of Synod approval**]. The Synod's resolution [**Reference number**] authorized the implementation of the Data Protection Policy across the Province of the Anglican Church of Kenya.

Authorized Signatories:

The Most Rev. Dr. Jackson Ole Sapit,
Archbishop – *Chairperson of the Provincial Synod*

Rt. Rev. Prof. Joseph Galgalo,
Provincial Secretary – *Secretary to the Provincial Synod*

(Note: Original signed copy of this Policy is archived with the Provincial Secretary's office. Copies may be distributed to all Dioceses and ACK institutions for implementation.)

List of Abbreviations and Acronyms

- ACK: Anglican Church of Kenya
- DPO: Data Protection Officer
- ODPC: Office of the Data Protection Commissioner
- DPA: Data Protection Act
- MoU: Memoranda of Understanding
- EU: European Union
- GDPR: General Data Protection Regulation
- PBO: Public Benefit Organizations
- SAR: Subject Access Request
- DPIA: Data Protection Impact Assessments
- CCTV: Closed-Circuit Television
- KRA: Kenya Revenue Authority
- USD: United States Dollar

Introduction

2.1 Introduction

The Anglican Church of Kenya (ACK) is committed to upholding the dignity, privacy, and trust of all individuals whose personal data it handles. In an age of digital information and heightened privacy concerns, this Data Protection Policy provides a comprehensive framework for how ACK collects, uses, stores, and protects personal data. It has been developed in alignment with ACK's mission and theological values, Kenya's Data Protection Act, 2019, and international best practices in data protection. Notably, Kenya's Data Protection Act, 2019 gives effect to the constitutional right to privacy (Article 31) and draws on global standards like Europe's GDPR. Churches and faith-based institutions are not exempt from these regulations – the law affects how churches handle member data and even activities like photographing congregants, which may require consent. This policy therefore ensures ACK's compliance with legal obligations while reflecting our Christian ethos of respect, stewardship, and justice.

This document is structured into clearly numbered chapters for easy reference. It will serve as ACK's institutional point of reference on data protection matters across all levels – from the Provincial Synod and Standing Committee to dioceses, parishes, and various institutions (such as Anglican Development Services, church schools, hospitals, and theological colleges). By implementing this policy, ACK seeks to honour the trust placed in it by clergy, members, staff, students, and all stakeholders, and to safeguard personal information as an expression of our commitment to love and justice. The policy is intended for formal adoption by the Provincial Synod, after which it shall be binding on all ACK entities and personnel.

Legal and Policy Framework

2.1 National Legal Framework in Kenya

Kenya's commitment to data protection is rooted in its Constitution and detailed in national law. The Constitution of Kenya (2010) explicitly guarantees the **right to privacy**. Article 31 of the Constitution provides that ***"Every person has the right to privacy, which includes the right not to have... information relating to their family or private affairs unnecessarily required or revealed, or the privacy of their communications infringed."***. This constitutional right establishes a broad principle that personal information must be safeguarded from unwarranted disclosure or intrusion.

To give effect to Article 31, Kenya enacted the **Data Protection Act, 2019** (DPA) as the primary statute governing personal data. The DPA came into force on 25 November 2019 and mirrors many international best practices (drawing on frameworks like the EU's GDPR) to protect individuals' personal data. It establishes definitions for key terms (such as "personal data", "data controller" and "data processor") and sets out the obligations of any person or organization handling personal data. Crucially, the DPA operationalizes Article 31(c) and (d) of the Constitution, protecting against the unlawful collection or revelation of private information and ensuring privacy of communications. Under the Act, data may only be processed (collected, used, stored, or shared) in compliance with a set of **data protection principles** and lawful bases. These principles require, for example, that personal data be processed lawfully, fairly and transparently; collected for explicit and legitimate purposes and not further used in incompatible ways; and be adequate, relevant, and limited to what is necessary for those purposes. They also mandate data accuracy, integrity and confidentiality (security), and accountability by data controllers. Data subjects (the individuals whom the data concerns) are given enforceable rights under the DPA – including the right to be informed about how their data is used, to access their own personal data, to request correction or deletion of inaccurate data, and to object to or restrict certain processing. These rights echo global norms of **Fair Information Practices**, such as those outlined in the United Nations Guidelines for the Regulation of Computerized Personal Data Files (1990).

Importantly, Kenya's law recognizes categories of sensitive personal data (for example, data about one's health status, religion, ethnicity, or children's data) that receive additional protection. The DPA requires extra safeguards or consent for processing such sensitive data, aligning with the principle of non-discrimination and special care for vulnerable persons' information. Overall, the national legal framework imposes a duty on the Anglican Church of Kenya (ACK) – like all organizations – to handle personal data with confidentiality, integrity, and respect for the individuals' privacy and dignity, as a matter not only of legal compliance but also constitutional right.

2.2 Regulations and the Data Protection Commissioner

The Data Protection Act established the **Office of the Data Protection Commissioner (ODPC)** to oversee and enforce data protection laws in Kenya. The ODPC (headed by the Data Commissioner) is empowered to ensure organizations comply with the DPA, to receive and investigate complaints from the public, and to take enforcement action in case of breaches. Following the Act's passage, a set of supporting regulations were developed to provide more detailed rules and procedures:

2.2.1 Data Protection (General) Regulations, 2021

General regulations elaborate on various aspects of the law, including details on data subject rights (e.g. how to obtain consent and facilitate access/correction requests), obligations of data controllers and processors, data protection impact assessments (DPIAs), personal data breach notifications, and restrictions on the commercial use of personal data. These regulations also outline requirements for **transfer of personal data outside Kenya**, specifying conditions under which cross-border transfers are permitted. Notably, the DPA and General Regulations highly regulate any transfer of personal data outside Kenya: a data controller/processor must prove to the ODPC that adequate safeguards are in place or that the destination country has comparable data protection laws, among other conditions. In the case of **sensitive personal data**, the data subject's explicit consent is required before transferring such data abroad. This means ACK must carefully assess any plans to store church members' or employees' personal information on servers or services located outside Kenya, to ensure compliance with these transfer restrictions.

2.2.2 Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021

sets out how individuals can lodge complaints with the ODPC and how those complaints will be handled. They detail the process for investigations, hearings, and enforcement orders in the event an organization (data controller or processor) is found to have breached the Act. For example, if a church member feels their data was misused or inadequately protected by an ACK office, they can file a complaint to the ODPC under these procedures. The ODPC can then investigate and, if necessary, issue enforcement notices or penalties. Non-compliance with an enforcement notice is an offence that can attract fines up to Kes 5 million or imprisonment, emphasizing the seriousness of these obligations.

2.2.3 Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021

Establishes a mandatory registration regime for certain data controllers and processors with the ODPC. The regulations empower the Data Commissioner to prescribe thresholds and criteria for registration. In general, organizations that handle large volumes of personal data or sensitive categories of data must register and obtain a certificate from the ODPC. As of early 2022, the threshold for **mandatory registration** was set such that any data controller or processor with an annual turnover below Kes 5 million (approximately USD $40,000) and fewer than 10 employees is *exempt* from mandatory registration. However, **certain types of organizations and activities must register regardless of size**. These include institutions involved in education, health services, financial services, telecommunications, transportation, and other areas considered high-impact or sensitive. For instance, an ACK diocesan secondary school or a church-run health clinic would *have* to register with the ODPC as data controllers due to processing student or patient data, even if their revenues or staff are below the threshold. Registration entails applying via the ODPC's online portal and paying a prescribed fee. Once registered, the entity receives a certificate (valid for 2 years) and is listed in the official register of data controllers/data processors. This process enables the ODPC to know which organizations are handling personal data and to oversee their compliance more effectively.

All three sets of regulations were gazetted and became effective by 14 February 2022 (with the Registration Regulations coming into force slightly later, on 14 July 2022). Together, the Act and Regulations give the ODPC robust tools to regulate data protection. The ODPC can

conduct audits of organizations, issue administrative fines or sanctions, and even refer serious offences for prosecution. It has also published guidance notes and manuals to help organizations comply. For example, the ODPC has released guidance on conducting Data Protection Impact Assessments, on obtaining valid consent, and sector-specific guidance such as for the **Education sector** and the **Health sector**. The education-sector guidance helps schools and training institutions (including church-run schools) understand how to handle students' personal data lawfully, covering issues like parental consent for minors and use of student records. The health data guidance similarly instructs hospitals and clinics on handling patients' health information with confidentiality and security. These tools are highly relevant to ACK's ministries in schooling and healthcare, and ACK is expected to follow such best practices.

2.3 International and Comparative Frameworks

While operating under Kenya's laws, ACK's approach to data protection also considers broader international principles and the practices of global church and nonprofit institutions. Data privacy is a universally recognized aspect of human rights. For instance, the **Universal Declaration of Human Rights (1948)** affirms that ***"No one shall be subjected to arbitrary interference with their privacy, family, home or correspondence"*** **(Article 12),** establishing privacy as a fundamental human right worldwide. In the decades since, many countries and organizations have developed convergent standards for protecting personal information.

One influential standard is the **European Union's General Data Protection Regulation (GDPR)**. Enacted in 2018, the GDPR is often considered a global "gold standard" for data protection. It introduced stringent requirements on transparency, consent, data minimization, and user rights, along with stiff penalties for non-compliance. GDPR's influence has been felt beyond Europe; Kenya's DPA 2019 was itself inspired in part by the GDPR's principles, ensuring concepts like lawful processing, purpose limitation, and data subject rights are well-aligned with international best practices. Although GDPR does not directly apply to ACK's domestic operations, it becomes relevant if ACK were to handle personal data of individuals in the EU or engage with international partners who require GDPR-level protections. Moreover, GDPR has set a benchmark that many global religious institutions strive to meet as a matter of good practice. For example, the Church of England (the mother church of the Anglican Communion, under UK/EU law) responded proactively

to GDPR by bolstering its data protection measures. The Church of England has noted that caring for personal data is an extension of the church's duty of care, stating that **"we take care of people's data and aim to be good stewards of it"**. This notion of **stewardship of personal data** – treating information entrusted to the Church with the same responsibility as one would treat other resources given by God – is a resonant concept across the Anglican Communion.

In addition to GDPR, Kenya and ACK are guided by other international instruments. The **United Nations Guidelines for the Regulation of Computerized Personal Data Files** (adopted by General Assembly resolution 45/95 in 1990) provide a set of foundational principles for data protection. These UN guidelines emphasize fairness, lawfulness, accuracy, purpose-specification, security, and the individual's right to access and correct their data – principles which are reflected both in Kenya's DPA and in ACK's own emerging policies. They also highlight the need for an independent supervisory authority and caution against abusive collection of sensitive data, underpinning the importance of regulators like the ODPC. Furthermore, the UN guidelines endorse **transborder data flow** protections, advising that personal data should freely flow between countries only if **comparable safeguards** exist in each. This concept is mirrored in Kenya's law, which, as noted, restricts cross-border data transfers to jurisdictions with adequate data protection or where other safeguards (or consent) are in place.

For ACK, being a faith-based and nonprofit institution, it is also useful to consider frameworks and guidance specific to such sectors:

- Globally, many **non-governmental organizations (NGOs)** and churches have adopted data protection policies that align with national laws and donor expectations. Donor agencies and international partners increasingly require Public Benefit Organizations (PBO) (including faith-based ones) to have strong data governance practices, especially when handling data of beneficiaries (e.g. community members, children, aid recipients). Although Kenya's ODPC has not issued church-specific rules, the general principles apply equally. In fact, protecting personal data is part of the broader **"good governance"** and accountability standards for nonprofits. ACK's compliance with data protection law thus complements its Christian witness by demonstrating transparency and respect in all administrative practices.

- Within Kenya, the ODPC's sector guidance for **education and health** are particularly pertinent since ACK operates schools, theological colleges, medical clinics, and hospitals. These guidance notes interpret the DPA in contexts like student records and patient health records. For example, they stress obtaining proper consent from parents or guardians when collecting information on minors in Sunday schools or youth programs and maintaining strict confidentiality of counselling or medical information obtained through pastoral care or health ministries. ACK is expected to follow such guidance to ensure it meets the heightened standards of care in these sensitive areas.
- In the international Anglican Communion context, churches have shared best practices on data protection. The Anglican Communion Office and various provincial churches have recognized that legal compliance in this area is part of the Church's **ethical responsibility**. Following the GDPR, numerous Anglican provinces (e.g. the Church of England, Anglican Church of Australia, etc.) either updated or formulated data protection policies. These often include practical measures like appointing Data Protection Officers, training clergy and staff in privacy principles, and publishing privacy notices for congregants and those who interact with church programs. By drafting this Data Protection Policy and its accompanying chapters, ACK joins those global Anglican peers in articulating both the legal requirements and the moral commitments involved in handling personal data.

Theology and Philosophy of Data Protection

3.1 Human Dignity and Respect for Privacy

The Anglican Church of Kenya approaches data protection not only as a legal duty but as a theological and moral imperative. At the heart of this perspective is the Christian belief in the **inherent dignity of every human being**, made in the image of God. In the Book of Genesis, we learn that God created humankind in His own image (Genesis 1:27), imparting to each person a sacred worth. This theological truth undergirds our respect for individuals' privacy and personal life. If every person bears God's image, then treating their personal information with care and confidentiality is a way of honouring that God-given dignity. Revealing someone's private matters without necessity or consent can amount to treating a person as a means rather than an end, thus failing to respect the divine image in them. By contrast, safeguarding personal data aligns with the **Christian respect for personhood** and the scriptural mandate to love our neighbour as ourselves – we guard others' information as we would want ours to be guarded.

Privacy, in a Christian sense, is linked to the notion of personal sovereignty and integrity granted by God. The **Constitution of Kenya** captures this in secular terms (protecting someone's home, communications, and private affairs from intrusion), but the Church sees an even deeper layer: each person has a God-given right to a degree of privacy, to solitude, and to control over their own story. Throughout the Bible, we find acknowledgments of appropriate privacy. For example, Jesus himself at times sought solitude or advised discretion. In the Gospels, after performing certain miracles, Jesus ***"often instructed those He healed not to tell anyone about it"*** (e.g. Mark 1:44, where He tells a healed leper ***"See that you say nothing to anyone"***). This could be understood as Jesus managing the spread of information for wise purposes – an implicit recognition that information should sometimes be kept confidential or shared only with the right people at the right time. Moreover, Jesus taught in Matthew 6 about doing acts of charity or devotion in secret without public display (Matthew 6:1-4), affirming that not everything in a person's life is meant for public exposure; there is virtue in **privacy, humility, and confidentiality**.

Anglican theology also emphasizes **freedom and autonomy** as aspects of human dignity. For individuals to exercise free will and moral responsibility (key traits of being made in

God's image), they need a sphere of privacy – freedom from constant surveillance or misuse of their personal information. In today's digital age, personal data is an extension of the person. Thus, respecting someone's data privacy is akin to respecting their personal boundaries and freedom to be themselves without undue interference. The misuse of personal data – say, for manipulation, commercial exploitation, or public shaming – can undermine a person's autonomy and dignity. It is notable that even in secular commentary, privacy has been called *"the foundation of democracy"* and crucial for individuals to act as independent moral agents. The Church resonates with this view; we see protecting privacy as creating space for people to develop and serve God free from coercion or fear. In short, **data protection is rooted in our belief in human dignity**: every name, every story, every piece of personal information entrusted to the Church is about a real person loved by God and must be handled with reverence and respect.

3.2 Stewardship, Trust, and Justice

In Anglican Church, the concept of **stewardship** is paramount. We believe that God entrusts us with resources – time, talent, treasure, and information – to use wisely and justly for His glory. Personal data can be viewed as another kind of resource that the Church might hold in trust. Whether it's baptismal records, counselling notes, or employee files, this information is not owned by the Church; it is entrusted to us by individuals and ultimately by God. Therefore, the ACK must act as a **faithful steward** of personal data. Being a good steward means we ensure data is used only for the legitimate ministry purposes for which it was collected and not for selfish or improper ends. It also means we protect data from loss, corruption, or unauthorized access – much as the Parable of the Talents teaches us to safeguard and responsibly multiply what is entrusted to us (Matthew 25:14-30). The Church of England articulated this idea well during the adoption of GDPR, noting that churches should already be ***"applying good practices – we take care of people's data and aim to be good stewards of it"***. By following robust data protection practices, ACK demonstrates **integrity in stewardship**, ensuring that the personal information of congregants, staff, students, or donors is handled in a way that honours God's trust and the trust of the people who have given us their data.

Hand in hand with stewardship is the value of **relational trust**. The ministry of the Church is profoundly relational – built on trust between clergy and laity, between the church and the wider community. Parishioners share personal details with clergy during counselling or

confession; families provide sensitive information when seeking pastoral services; employees and volunteers trust the church with their personal records. Maintaining strict confidentiality and data security is essential to preserving this sacred trust. Proverbs 11:13 observes that ***"A trustworthy person keeps a secret, but a gossip goes about revealing matters."*** This wisdom from Scripture underscores that keeping confidences is a virtue, whereas careless disclosure can cause harm and erode relationships. For ACK, a data breach or misuse of information wouldn't just be a legal issue – it would be a **breach of trust and pastoral ethics**. By implementing strong privacy measures, the Church communicates to its members: ***Your information is safe with us; we will not betray your confidence.*** This assurance encourages openness and honesty in pastoral conversations and church life, because people know their personal vulnerabilities or prayer requests won't become public gossip. In this way, data protection supports the Church's pastoral mission, fostering an environment of **safety, respect, and trust** where individuals can be ministered to more effectively.

Stewardship and trust also extend to **justice and protection of the vulnerable** – core concerns in Christian teaching. Throughout Scripture, God calls His people to protect the widow, the orphan, the stranger – those who are vulnerable or powerless (e.g. Psalm 82:3, James 1:27). In the modern context, misuse of personal data can disproportionately harm the vulnerable: for instance, a breach of a children's ministry database could put minors at risk, or improper handling of welfare recipients' data could lead to stigma or fraud. The Church's commitment to justice means we must be vigilant to prevent such harms. The **Five Marks of Mission** of the Anglican Communion include ***"to respond to human need by loving service"*** and ***"to transform unjust structures of society, to challenge violence of every kind, and pursue peace and reconciliation".*** These Marks remind us that defending people's rights and well-being is part of our mission. Applied to data protection, this implies advocating for equitable treatment of individuals' data and resisting any abusive data practices. For example, it would be unjust for personal data to be collected from parishioners under false pretences or used to exploit them. It would likewise be unjust if the privacy of, say, an HIV-positive church member or a survivor of abuse in our congregation was violated through careless data handling, potentially leading to social ostracism or emotional trauma. Therefore, ACK's data protection efforts are a matter of **justice** – ensuring that we do not become party to the exploitation or harm of the people we serve, especially those who are most vulnerable. As one Anglican ethical guidance on technology investment noted, Christians are ***"called to stand with the marginalised... God cares for the smallest,***

the weakest and the least powerful." In practical terms, that means our data policies must pay special attention to protecting children, the elderly, the sick, the poor, and any whose personal information, if misused, could put them at risk. We put in place appropriate safeguards (like obtaining informed consent, limiting who can access sensitive files, and anonymizing data where possible) out of a biblical mandate to **"defend the rights of the poor and needy"** (Prov. 31:8-9) even in the digital realm.

3.3 Anglican Teachings and the Digital Age

Anglicanism has a rich tradition of engaging with the ethical challenges of each era, seeking to apply timeless Christian principles to contemporary issues. The digital age – with its vast capabilities for data collection and surveillance – is no exception. The global Anglican Communion has increasingly recognized that technology and data ethics are areas requiring the Church's active reflection and guidance. As far back as the 1998 Lambeth Conference (the decennial gathering of Anglican bishops worldwide), church leaders foresaw the importance of grappling with technological change. **Lambeth 1998 Resolution I.12** called for the establishment of a commission to **"track technological developments, to reflect on them theologically and ethically, and to inform bishops and other church leaders"** of relevant insights. This was a proactive acknowledgement that emerging issues – like digital privacy, bioethics, or internet usage – should be examined through a faith lens. In more recent years, Anglican bodies such as the Anglican Consultative Council and various provincial synods have produced statements on human dignity in the digital realm. For example, Anglican representatives have spoken at global forums about artificial intelligence and data ethics, emphasizing values like transparency, accountability, and human-centered technology in line with Christian teaching. The Church is adding its voice to ensure that advancements in "Big Data" and "Big Tech" are aligned with the common good and the **infinite dignity of every person**, rather than solely driven by profit or power. (Other ecumenical partners have echoed such concerns, noting that *"the protection and preservation of human dignity must extend into the digital realm"*.)

Within ACK's context, we align with the broader Anglican Communion in affirming that **ethics must guide technology**. We view data protection as part of the Church's witness in society – modelling what it means to treat people justly and lovingly. ACK's own doctrines and synodal teachings reinforce this stance. The Church's mission statement is ***"to equip God's people to transform society with the Gospel",*** a holistic transformation that

"addresses our deepest need... a restored relationship with the God in whose image we are made". A society transformed by the Gospel is one where human dignity is upheld, and unjust exploitation is challenged. Thus, advocating for privacy rights and ethical data use in Kenya can be seen as part of "transforming unjust structures of society" (an echo of the Fourth Mark of Mission). In a world where personal data can be misused for injustice – from identity theft and fraud to surveillance and suppression of freedoms – the Church has a role in promoting what is right. We support laws and practices that curb data abuses, and we commit to internal standards that exceed mere compliance, embodying Christ-like care. By doing so, ACK contributes to a culture where technology serves humanity's God-given dignity and **not the other way around**.

Anglican social teaching also highlights the importance of **community and relationships**, which informs how we handle data. We are not just isolated individuals; we are part of the Body of Christ and members one of another. This communal outlook means that what we do with someone's personal information can affect the whole community's trust and cohesion. The biblical vision of society (shalom) is one where each person is valued and no one is exploited; privacy and reputation are protected so that community bonds remain strong. In practical terms, an ACK parish that diligently protects its members' data is likely to have a healthier community life – free from rumours, identity abuses, or breaches that sow fear. In contrast, if a church were careless with data (for instance, accidentally leaking the tithing records or health status of some members), it could create gossip, envy, or embarrassment that harm unity. Therefore, our data protection philosophy is also about **fostering right relationships** in the church. It resonates with Paul's teaching that the Church must handle matters "decently and in order" (1 Cor. 14:40) and with transparency and honesty (2 Cor. 8:21), which would include how we manage information. We aim to be a "safe church" – a term the Anglican Communion uses to describe a church that is safe for all, including in terms of safeguarding personal data and privacy. The Anglican Communion's **Safe Church principles** implicitly support confidentiality and respect for personal boundaries, complementing our data protection aims.

Finally, Anglican sacramental theology even provides insights: just as we treat the sacraments (like baptismal records or marriage registers) with reverence, understanding they pertain to holy moments in people's lives, so we treat all personal data with a sense of sacred responsibility. The Lambeth Conferences and other Anglican consultative bodies continually remind us that **mission and ministry must be carried out with integrity**. Data

protection is now part of that integrity. It's an area where the Church's Walk must match its talk – we cannot preach about love, respect, and justice on Sunday and mishandle personal information on Monday. By embedding theological values into our data protection policy, ACK ensures that our handling of data is an extension of our faith and discipleship.

3.4 Integrity, Pastoral Care, and ACK's Mission

For the Anglican Church of Kenya, implementing data protection is ultimately about **living out our Christian values in every administrative and pastoral action**. ACK has long emphasized principles of integrity, accountability, and servant leadership in its governance. Our commitment to protecting personal data is a natural extension of this ethos. It signals that the Church is **transparent and trustworthy** in how it conducts its affairs, which strengthens our witness to Christ. When church members and the public see that ACK respects privacy and guards' information, it reflects our wider commitment to honesty and care – ***"doing to others as we would have them do to us"*** **(Luke 6:31)**. In a society increasingly concerned with data breaches and privacy violations, the Church can be a beacon of assurance that people's information will not be exploited or treated carelessly within our institutions. This integrity in data handling also frees the Church to prophetically encourage other actors in society (like businesses or government) to likewise uphold high standards, without any hypocrisy.

Pastoral care is one of the most sensitive areas that benefits from strong data protection. Clergy and lay pastors often receive confidential information from individuals seeking counsel or support. Traditionally, the church has upheld confidences (for instance, the seal of confession in some Anglican contexts, or simply the ethical duty of a vicar not to disclose what is shared in private). In the modern regulatory environment, this traditional pastoral confidentiality aligns with data protection requirements. ACK's policy will ensure that information from pastoral interactions – whether notes from a counselling session, prayer requests that include personal details, or church disciplinary matters – are kept secure and only shared with those authorized and on a need-to-know basis. This is not merely about compliance, but about **love and respect** for the person who may be in a vulnerable state. It is our theological conviction that exposing someone's weakness or sin without cause is a failure of love (recall Noah's sons covering their father's nakedness in Genesis 9:23 as a sign of respect, whereas gossip or exposure would be dishonouring). By protecting such

data, we practice the *"love that covers a multitude of sins"* (1 Peter 4:8) – not to enable wrongdoing, but to allow people the space to repent, heal, and grow without public shame.

Moreover, ACK's mission to **"equip God's people to transform society with the Gospel"** includes equipping our own community with knowledge and ethical frameworks for the digital age. We will incorporate teachings about digital responsibility, cyber-awareness, and the Christian perspective on privacy into our discipleship programs where appropriate. For example, youth groups and parish forums can discuss biblical principles that apply to social media use or protecting one's personal information online. In doing so, we are helping form Christians who are thoughtful and morally grounded "digital citizens." This educational aspect connects to the Church's role in society: as Kenya continues to digitize (government services, communication, finance, etc.), the Church can provide moral guidance on how technology is used. Our data protection policy, grounded in theology, can serve as a model or reference point for other faith-based organizations in Kenya. It shows how one can **marry legal compliance with Christian ethics**, producing a policy document that speaks both the language of the law and the language of faith.

The theology and philosophy behind ACK's Data Protection Policy affirm that protecting personal data is part of **our calling to respect human dignity, exercise wise stewardship, and pursue justice and love**. The policy is not an external obligation reluctantly followed, but an internal commitment joyfully embraced – because it resonates with the Gospel values we cherish. As we implement this policy, we do so prayerfully and conscientiously, knowing that in protecting the privacy and personal data of those we serve, we are in fact protecting the *"least of these"* (Matthew 25:40) and honouring the God who created them. Our hope is that through this effort, the Church will continue to be seen as a trustworthy sanctuary in an age of constant data exposure – a community where people are known and cared for, but also **safe and respected in their personal information**. This integrity glorifies God and adorns the Gospel we proclaim.

Definitions

For clarity, the following definitions apply within this policy (drawn from the Data Protection Act, 2019 and ACK's context):

4.1 Personal Data:

Any information relating to an identified or identifiable natural person ("data subject"). This includes identifiers such as name, identification numbers, contact information, images, email addresses, biometric data, and any information that can be linked to a specific individual. It covers both information and opinions about a person. Examples in ACK context: baptismal records of a member, an employee's HR file, a student's report card, or a patient's medical record.

4.2 Sensitive Personal Data:

Personal data that is particularly private in nature, thus requiring extra protection. Under Kenyan law this includes data revealing a person's race, ethnic or social origin, health status, genetic or biometric data, religious or philosophical beliefs (conscience), mental status, marital status, family details (e.g., names of children or spouses), property details, sex life or sexual orientation. In ACK's context, information about someone's faith commitment, pastoral counselling notes, health information in church hospitals, or any detail that could be sensitive falls in this category. Such data must be handled with heightened care, often requiring explicit consent or other special safeguards.

4.3 Data Subject:

The individual whose personal data is processed. This can be anyone whose data ACK holds – e.g., a church member, a cleric, an employee, a student, a patient, a donor, or even a visitor whose details are recorded.

4.4 Data Controller:

A person or entity that determines the purpose and means of processing personal data. For purposes of this policy, ACK (through its governing bodies or institutions) is typically the Data Controller for data collected in its ministries. For example, the ACK Provincial Office is the controller of data in the central membership system; a Diocesan office is a controller for diocesan personnel records; a church hospital is controller of its patient data.

4.5 Data Processor:

A person or entity that processes personal data on behalf of a controller. This could be an ACK entity processing data for another (e.g., a diocesan office processing parish data) or an external service provider contracted by ACK. For instance, if ACK engages a cloud database service or an IT firm to manage its data, that external firm acts as a data processor and must adhere to our data protection requirements.

4.6 Processing:

Any operation performed on personal data, whether by automatic means or otherwise. This includes collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission or dissemination, alignment, combination, restriction, erasure, or destruction of personal data. In simple terms, anything we do with personal data – from the moment we receive it to the moment we delete it – counts as "processing".

4.7 Consent:

An indication of the data subject's wishes by which they signify agreement to the processing of their personal data. The Act requires consent to be ***"express, unequivocal, free, specific and informed"***. In practice, this means a clear affirmative action or statement by the individual. For ACK, consent might be obtained via signed forms or online checkboxes for specific purposes (e.g., consenting to receive a newsletter or to have one's photo published).

4.8 Child/Minor:

In line with Kenyan law, anyone under the age of 18 years. Special rules apply to processing personal data of children (see Chapter 12). Generally, consent or authorization from a parent or legal guardian is required to process a child's data, except in certain exceptional circumstances (such as safeguarding vital interests of the child).

4.9 ACK Institutions:

Refers collectively to all organizational units of the Anglican Church of Kenya, including but not limited to the Provincial offices, Dioceses, Parishes, Anglican Development Services (ADS) regions, church-run schools, colleges, health facilities, and any other boards, departments or ministries under ACK oversight. These are the entities to which this policy applies.

4.10 Data Protection Officer (DPO):

A person appointed to oversee data protection compliance within ACK. While not every organization is strictly required by law to have a DPO, it is recommended for those handling substantial or sensitive personal data. ACK may designate a DPO at the provincial level (and/or at diocesan levels) to coordinate compliance efforts (see Chapter 6.0 on Governance).

4.11 Data Breach:

A security incident leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data. For example, a data breach can occur if a laptop with unencrypted ACK data is stolen, if a database is hacked, or if confidential files are mistakenly sent to the wrong recipient. Breaches can compromise privacy and trigger legal duties to notify (see Chapter 10).

Unless otherwise defined here, terms used in this policy have the same meaning as in the Data Protection Act, 2019. These definitions ensure a common understanding for all readers and will guide the interpretation of the policy provisions that follow.

Scope and Applicability

This Data Protection Policy applies to **all personal data processed by the Anglican Church of Kenya and its institutions**. The scope is comprehensive and covers:

5.1 Entities Covered:

All levels of ACK's ecclesial structure – including the Provincial Synod and its Standing Committee, Provincial offices and Boards, all Dioceses and their offices, parishes and congregations, as well as affiliated or subsidiary organizations such as Anglican Development Services (regional development programs), church-sponsored schools, training centres, hospitals/clinics, theological colleges, and any other official institutions of ACK. Each of these entities is expected to adopt and implement this policy. Where necessary, local guidelines or procedures may be developed to operationalize this policy, but they must conform to the standards herein.

5.2 Personnel Covered:

All individuals handling personal data under ACK's auspices. This includes clergy (bishops, priests, deacons), lay leaders, employees (permanent, contract, casual), volunteers, interns, and any other persons who have access to personal information through ACK activities. Every such person has a duty to comply with this policy and will be held accountable for any data protection breaches.

5.3 Data Covered:

All forms of personal data, whether in electronic/digital format or in physical/manual form, processed by ACK. This ranges from church membership lists, sacramental registers, HR records, payroll and financial records, educational records, medical records, photographs and audio/video recordings of individuals, communication records (emails, letters involving personal details), to ID numbers and any other personal identifiers. Both structured data (e.g., databases, filing systems) and

unstructured personal data (e.g., free-form notes that are part of a filing system) are included.

5.4 Processing Activities:

The policy applies to the entire data lifecycle – collection, use, disclosure, storage, transmission, and disposal of personal data – conducted by or on behalf of ACK. It covers processing within Kenya as well as any cross-border processing (e.g., if an ACK database or cloud service is hosted outside Kenya, or if data is shared with an overseas partner, Chapter 13 on Third-Party and Data Sharing will apply).

5.5 Geographical Scope:

All ACK operations and ministries, whether within Kenya or, if applicable, outside Kenya, must comply. If ACK engages in activities across the border (for example, a mission in another country or interacting with the global Anglican Communion involving personal data exchange), those activities should be governed by this policy in addition to any local laws. Importantly, personal data transferred out of Kenya is subject to Kenya's cross-border transfer rules (requiring safeguards or consent), so any such transfers must be carefully managed (see Chapter 13).

5.6 Exclusions:

This policy does **not** apply to purely personal or household activities by individuals (for instance, a private address book of a clergy member used personally). It also does not cover anonymous or fully anonymized data that cannot be linked to an individual (once data is truly anonymized such that the person is not identifiable, it is no longer "personal data" by definition). However, if anonymized data could be re-identified, it should still be treated as within scope.

Governance Structure and Responsibilities

Effective data protection requires clear governance and assignment of responsibilities at every level of the Church's structure. ACK's governance model for data protection is as follows:

6.1 Oversight by Provincial Synod and Standing Committee:

The Provincial Synod of the Anglican Church of Kenya, as the Church's highest governing body, shall approve this Data Protection Policy and any significant amendments. The Standing Committee of the Provincial Synod (which acts on behalf of Synod between its sessions) will provide ongoing oversight of its implementation. The Standing Committee will receive periodic reports on data protection compliance across the Church and may issue additional guidelines or allocate resources as needed to support compliance. In line with its mandate, the Standing Committee ensures that ACK's data protection efforts align with our mission and legal obligations, treating this as a top-level governance issue akin to financial or doctrinal integrity.

6.2 Provincial Data Protection Officer (DPO) or Compliance Unit:

ACK shall designate a Data Protection Officer at the Provincial level (or establish a Data Protection Compliance Committee/Unit) to coordinate and support compliance efforts church wide. The DPO (or equivalent) will be a person with appropriate expertise in data privacy law and practices and will report to the Provincial leadership (the Provincial Secretary). Key responsibilities of the DPO include advising ACK and its institutions on data protection obligations, monitoring compliance with this policy and the law, conducting or facilitating training (see Chapter 14 Compliance and Training), and serving as the contact point for the ODPC and data subjects on privacy matters. The DPO will also guide any required Data Protection Impact Assessments (DPIAs) for new projects that may pose high privacy risks and will assist in handling data breach response (see 10). Having a DPO

demonstrates ACK's commitment to compliance and helps reduce risk of breaches or penalties.

6.3 Diocesan and Institutional Responsibilities:

Each Diocese shall be responsible for implementing this policy within its jurisdiction. The Diocesan Bishop, in collaboration with the Administrative Secretary (or another appointee), must ensure that parishes and diocesan departments comply. It is recommended that each Diocese appoints a Data Protection Compliance Coordinator (which could be an existing staff role, such as the Diocesan Secretary or IT Officer) to liaise with the Provincial DPO and oversee local compliance (e.g., maintaining records of data processing at the diocesan level, coordinating responses to data subject requests in that diocese, etc.). Similarly, every ACK institution (schools, hospitals, ADS programs, etc.) should designate a responsible person (e.g., school principal, hospital administrator, program director) for data protection. That person must ensure the unit follows this policy – including secure data handling, staff awareness, and reporting any issues up to the Diocese or Provincial DPO.

6.4 Parish and Local Level:

At the parish level, the Vicar/Priest-in-Charge together with the Parish Council bear responsibility for protecting personal data of parish members and community. They must ensure that membership records, sacramental registers, and any other personal data (e.g., photos taken at parish events, personal details of those seeking aid, etc.) are collected and used in line with this policy. Parishes should handle data subject requests (like a member asking to update their contact info or opt out of certain communications) promptly, with guidance from the diocese if needed. Volunteers or lay leaders who handle personal data (Sunday school teachers with children's info, lay readers visiting homes with personal notes, etc.) should be instructed on confidentiality and required to comply with the policy. Parishes are often the first contact point for individuals, so they should also communicate

privacy notices to congregants (e.g., informing members how their data will be used by the church).

6.5 Boards and Committees:

Various boards and committees within ACK (e.g., boards of education, health boards, the Provincial Board of social services handling donor data, etc.) must also observe data protection principles. If such bodies process personal data (for example, the education board handling scholarship student data, or a committee managing a list of partners), they are responsible for that data's protection. Chairs of these Boards should ensure discussions or documents containing personal data are handled securely (e.g., minutes carefully without unnecessary personal details, stored properly).

6.6 Individual Responsibilities and Confidentiality Duty:

Every clergy member, staff, or volunteer with access to personal data has an individual responsibility to safeguard it. This includes following procedures for data security (Chapter 10), respecting confidentiality (not disclosing data to unauthorized persons, even informally), and reporting any suspected data breach or misuse promptly through the proper channels. Unauthorized disclosure of personal data by any member of ACK could lead to disciplinary action and legal consequences. All clergy and staff, upon appointment or hiring, should sign a commitment to uphold confidentiality and data protection rules as part of their terms of service.

6.7 Office of the Data Protection Commissioner (ODPC) Interactions:

The Provincial DPO or designated officer will act as the primary liaison with Kenya's ODPC. ACK will comply with requirements such as registration of data controllers/processors if meeting the prescribed thresholds (for instance, if volume of data or sensitive data handled exceeds ODPC's registration criteria, the Provincial office and relevant institutions will register as required). The ODPC has authority to conduct audits and inspections; ACK's policy is to cooperate fully and transparently

with the regulator. Any official communication to or from the ODPC (e.g., inquiries, complaints forwarded, breach notifications) should promptly involve the Provincial DPO and ACK legal advisors.

Data Protection Principles

ACK affirms and adopts the core principles of data protection as laid out in the Data Protection Act, 2019. These principles guide all our personal data processing activities and serve as the foundation for specific practices described later in this policy. Every data controller or processor within ACK must ensure that personal data is handled in accordance with these principles:

7.1 Right to Privacy:

"Personal data shall be processed in accordance with the right to privacy of the data subject". ACK recognizes privacy as a fundamental human right. This means we approach personal data handling in a way that upholds an individual's privacy and confidentiality. Any action we take with someone's data should consider their dignity and reasonable expectations of privacy, consistent with our theological ethos and constitutional rights.

7.2 Lawfulness, Fairness and Transparency:

All personal data must be processed ***"lawfully, fairly and in a transparent manner"*** in relation to the individual. *Lawfulness* means ACK will only process data if there is a valid legal basis (see Chapter 8.0) and in compliance with all applicable laws. *Fairness* means we will not use data in ways that unjustly harm or surprise individuals; our actions with data should be ethically sound and considerate. *Transparency* means we will be open with data subjects about our data practices – informing them what data we collect, for what purposes, and with whom it is shared. For example, when someone joins a parish, we will provide a privacy notice explaining how their information will be used by the church.

7.3 Purpose Limitation:

Personal data shall be ***"collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes".*** ACK will

clearly define the purposes for which data is collected (e.g., pastoral care, sacramental records, payroll, alumni relations for a school, etc.), and we will not use the data for any new or unrelated purpose without obtaining consent or ensuring it aligns with an allowed exception. If we collect someone's address for sending a church formal communication, we will not suddenly use that address for, say, commercial marketing or unrelated activities without consent. Any additional use of data must be evaluated for compatibility or requires fresh consent from the data subject.

7.4 Data Minimization:

We will ensure that personal data collected is *"adequate, relevant, and limited to what is necessary"* in relation to the purposes for which it is processed. In practice, ACK and its institutions will only ask for and keep the personal information that we truly need. Extraneous or overly intrusive data collection is avoided. For instance, a parish registration form will ask for contact and basic demographic info needed for ministry but will not request unnecessary details about one's family unless there is a justified reason. By minimizing data, we reduce the risk of misuse and respect individuals' privacy by not prying into aspects of their lives unrelated to the church's legitimate purposes.

7.5 Valid Explanation for Certain Data:

The law specifies that data should be ***"collected only where a valid explanation is provided whenever information relating to family or private affairs is required"***. ACK interprets this to mean if we need to collect sensitive personal details (for example, information about a person's family members, marital situation, or private matters), we will explain why this is needed and ensure the individual understands the reason. We will not collect deeply personal information (such as marital counselling notes, or details about a member's personal struggles) without context, consent, and assurances of confidentiality. This principle underscores respect for the intimate nature of certain data and requires justification for its collection.

7.6 Accuracy:

ACK will keep personal data *accurate and up-to-date*, and *"every reasonable step"* will be taken to ensure that inaccurate data is corrected or deleted *"without delay"*. We rely on individuals to provide accurate information, but we will also facilitate updates. For example, if a congregant informs us their name was misspelled or their contact number changed, we will promptly update our records. Regular audits of key databases may be conducted to purge or fix outdated or incorrect entries. Inaccuracies can lead to harm (imagine sending confidential letters to the wrong address), so maintaining accuracy is an ethical and legal imperative. Data subjects have the right to rectification of their data, which we fully uphold (see Chapter 9.0).

7.7 Storage Limitation:

Personal data shall be ***"kept in a form which identifies the data subjects for no longer than is necessary"*** for the purposes for which it was collected. ACK will establish retention periods for different categories of data (see Chapter 11.0). We will not keep personal data indefinitely "just in case" – except in instances where archival retention is in the public interest or historical interest (for example, church registers that have historical value may be kept long-term securely, but even then, the use of such archived data will be limited). Once the purpose is fulfilled and no legal requirement compels retention, we will securely dispose of or anonymize the data. This principle helps prevent accumulation of stale data that could pose security risks or infringe on privacy over time.

7.8 Integrity and Confidentiality (Security):

Personal data must be *secured against unauthorized or unlawful processing, and against accidental loss, destruction, or damage*. ACK will implement appropriate technical and organizational measures to ensure the security of personal data (detailed in Chapter 10.0). Confidentiality means only authorized persons should access or handle personal information. Integrity means maintaining the consistency, accuracy, and trustworthiness of data (preventing improper alteration or corruption). Whether the data is in digital form (protected by passwords,

encryption, etc.) or physical form (kept in locked files, not left unattended), we will strive to protect it from breaches. We acknowledge that the Church, like any organization, can be target of data theft or prone to errors – thus robust safeguards and a culture of confidentiality are non-negotiable.

7.9 Cross-Border Transfer Limitation:

ACK will not transfer personal data outside Kenya unless there is proof of adequate data protection safeguards, or the data subject has given consent. Kenya's law highly regulates cross-border data transfers (Part VI of the Act) – requiring controllers to demonstrate that the foreign country or receiving entity has commensurate data protection or appropriate contractual safeguards. In addition, transfer of *sensitive personal data* out of Kenya specifically requires the data subject's consent. Therefore, if any ACK institution needs to use cloud servers or share data with an overseas partner (like an international Funding Partner or the wider Anglican Communion office), we will first ensure compliance with these conditions. Usually, this will involve either using data centres in jurisdictions with strong privacy laws or obtaining explicit consent from individuals. All cross-border transfers must be approved by the Provincial DPO or relevant authority to ensure legal compliance.

7.10 Accountability:

Although not listed as a separate principle in the Act's section 25, the principle of accountability is central to data protection governance. ACK acknowledges its accountability for all personal data under its control. We will ***"take responsibility for personal data and ensure individuals can exercise their rights, while providing clear information on data processing"***, in line with best practice. This means ACK must not only abide by these principles but be able to demonstrate compliance (e.g., through documentation, training records, audit logs). Each level of ACK's hierarchy is answerable for upholding these standards. We cannot delegate away the ultimate responsibility – even when using third-party processors, ACK remains accountable to data subjects and regulators for proper data handling.

Lawful Basis for Processing

ACK will only process personal data if at least one of the lawful bases (legal justifications) for processing, as defined in the Data Protection Act, is satisfied. Before collecting or using any personal data, we will determine which of the following bases applies:

8.1 Consent of the Data Subject:

Where feasible and appropriate, ACK will seek the free, informed, and explicit consent of the individual for specific processing. Consent is typically required for activities that are not obviously part of our core relationship with the person. For example, a parish may ask for consent to use a member's photograph on the church website, or a school may request parental consent to share a student's story in a newsletter. Consent will be documented (via signed forms or electronic records) and individuals have the right to withdraw consent at any time. We will avoid "bundled" or assumed consent; instead, we will clearly specify what the person is agreeing to. If consent is withdrawn, we will cease the processing unless another lawful basis applies.

8.2 Contractual Necessity:

Processing is lawful if it is ***"necessary for the performance of a contract to which the data subject is a party, or to take steps at their request prior to entering a contract"***. In an ACK context, this can apply to employment contracts (we must process employees' data to pay salaries, provide benefits, etc.), student admissions (processing data when a student enrols in a church-run school/college under an enrolment agreement), or service contracts (if someone rents church premises, their details are processed as part of that agreement). We will limit such processing to what is necessary for the contract – for example, an employee's bank details are needed for payroll, but we wouldn't collect data not relevant to the employment contract.

8.3 Legal Obligation:

We may process personal data if it is ***"necessary for compliance with a legal obligation to which the controller is subject"***. ACK, as a registered institution, has various legal obligations – e.g., statutory reporting to the government, compliance with court orders, tax law (like providing KRA with PAYE details for staff), or obeying public health directives. When we process data to meet such obligations, that is a lawful basis. For instance, if the law requires us to provide certain records for an audit or an official census of churches, we will do so in line with that obligation. We will ensure that only the required data is shared and that the request is legitimate.

8.4 Vital Interests of the Data Subject (or Another Person):

In emergencies, ACK may process personal data as necessary ***"to protect the vital interests"*** of the individual or another person. "Vital interests" means matters of life and death or grave bodily harm. For example, if someone is injured during a church event and unconscious, church staff may share known medical information about that person with paramedics without consent, if that information could save their life. Similarly, our hospitals might use patient information in a critical situation to protect someone's life. This basis is only used in urgent, critical situations where other bases (like consent) cannot be obtained in time.

8.5 Public Interest / Official Authority:

The Act recognizes processing that is ***"necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller",*** as well as processing by public authorities or for functions of a public nature. ACK is not a government body, but some of our activities can be considered as carried out in the public interest or for charitable common good – for instance, running schools, hospitals, or relief efforts. In certain cases, those activities might justify data processing under this basis, especially when delivering services for public benefit (such as collecting personal details for a relief distribution list). However, since ACK is fundamentally a private charitable/religious entity, we will typically rely on consent or legal obligation rather than assume "official authority."

If we partner with government on a project (like a public health campaign through our hospitals), any data processing on that project might fall under this category in coordination with the authorities.

8.6 Legitimate Interests:

It is lawful to process data for the *"legitimate interests"* pursued by the data controller or a third party, except where such interests are overridden by the data subject's rights and freedoms. This basis requires balancing ACK's legitimate aims against the individual's privacy expectations. Many internal church processes can rely on legitimate interests. For example, ACK has a legitimate interest in maintaining a membership roll to shepherd its flock, or a diocese may have a legitimate interest in sharing a bishop's itinerary with parishes (using personal data of the bishop) for coordination. Likewise, using members' addresses to send them stewardship materials might be considered a legitimate interest of the church's mission. When using this basis, ACK will assess the impact on the individual – if the processing could be seen as intrusive or unexpected, we will either avoid it, provide a right to object, or use consent instead. Notably, the Act warns that if processing under legitimate interests would cause harm or prejudice to the individual's rights, it is unwarranted. We will document our "legitimate interests' assessments" for major uses of this basis, to show that we considered and mitigated risks to data subjects.

8.7 Historical, Statistical, Journalistic, Artistic or Research Purposes:

The law explicitly allows processing for *"historical, statistical, journalistic, literature and art or scientific research"* purposes, provided the processing is lawful and meets applicable safeguards. For ACK, this might be relevant in preserving archives (historical parish registers, archival research on church history), compiling statistics (like aggregated demographic data of membership for planning, without identifying individuals), or publishing newsletters and articles (journalistic/artistic). When processing data for these purposes, we will adhere to any conditions in the Act (for example, ensuring that published works do not infringe individuals' privacy without

consent, unless public interest justification exists). If using personal data in academic research or surveys, we will anonymize it where possible or obtain consent as needed.

In all cases, ACK will identify and record the lawful basis before or at the time of data collection. Individuals will be informed of the basis in the applicable privacy notice (for example, a church donation form might state “we process your data under our legitimate interest to issue receipts and acknowledge contributions” or an employment form might state “necessary for contract and legal obligations”). If the initial basis for processing changes (e.g., we originally relied on consent but later want to use the data under legitimate interest), we will evaluate legality and inform individuals or obtain new consent accordingly.

8.8 Special Category (Sensitive) Data:

Given that ACK handles sensitive personal data (especially data revealing religious belief, which is inherently involved in church membership, as well as possibly health data in our medical institutions), we recognize that processing such data often requires *explicit consent* or other specific conditions. The Act (section 45) provides additional grounds for sensitive data – including where the processing is carried out by a not-for-profit body (like a church) during its legitimate activities with appropriate safeguards and relates solely to members or persons in regular contact, and the data is not disclosed to outside parties without consent. ACK will ensure that any processing of sensitive data meets these strict conditions. For example, information on someone’s faith journey shared within a parish context will not be divulged externally without consent. Furthermore, when processing children’s sensitive data (like health or disability information in a church school), we will obtain parental consent and protect such data diligently.

Data Subject Rights

Every person whose data is held or processed by ACK (the “data subject”) has certain rights under the law. ACK is committed to upholding these rights and facilitating their exercise without undue delay or hindrance. The following are the key data subject rights recognized by the Kenyan Data Protection Act and affirmed by this policy:

9.1 Right to Be Informed:

Individuals have the right to be informed about the collection and use of their personal data. ACK will provide clear and accessible privacy notices whenever personal data is collected. This includes informing data subjects about the purposes of processing, the lawful basis being relied on, any third parties with whom data will be shared, the period data will be stored, and the rights the individual has (including how to exercise them). For example, a form for new church members or an online registration for an event will include a brief statement or link explaining how their data will be used. Transparency is crucial; we want our members, staff, and service users to know what happens with their information within the church.

9.2 Right of Access:

A data subject has the right to access personal data that ACK holds about them. Upon request, and after verifying the requestor’s identity, ACK will provide a copy of the individual’s personal data, as well as information on how it has been used, who it has been shared with, and the source of the data (if not collected directly). This is commonly known as a Subject Access Request (SAR). We will respond to access requests within the time frame specified by law (usually within 30 days) and at no charge for the first request (a reasonable fee may be charged for additional copies or manifestly unfounded/repetitive requests, as permitted by law). For example, a church employee can request to see the information in their HR file, or a parishioner can ask what contact details the parish holds for them.

9.3 Right to Rectification:

Individuals have the right to have inaccurate or incomplete personal data corrected. If a data subject discovers or notifies us that the data we hold is incorrect or outdated (e.g., name spelling, contact number, or any factual detail), ACK will rectify it as soon as possible. We may need to verify the correct information before making the change. If we have shared that data with third parties, we will inform them of the correction where feasible. Additionally, as a proactive measure, ACK encourages members and stakeholders to update their information regularly (for instance, a yearly update of parish rolls details). Keeping data accurate is both the individual's right and our responsibility.

9.4 Right to Deletion (Erasure):

The Act grants individuals the right to deletion of false or misleading data about them, and more broadly, data subjects can request deletion or erasure of personal data in certain circumstances – for example, if the data is no longer necessary for the purpose, or the processing was based on consent which has now been withdrawn (and no other lawful basis applies). ACK will honour valid requests for erasure. This could apply, for instance, when someone who had subscribed to a newsletter asks to be removed (we would delete their contact from our mailing list). However, it's important to note that this right is not absolute: we may refuse deletion where we have a compelling legitimate reason or legal obligation to retain the data (e.g., sacramental records which serve as legal documents, or employment records needed for labour law compliance). In case we cannot delete data that was requested, we will provide the individual with the reason (such as legal requirement) and, if applicable, restrict the data from active use.

9.5 Right to Object and Restrict Processing:

Data subjects have the right to object to the processing of all or part of their personal data, particularly for certain purposes like direct marketing. If ACK is processing data under a legitimate interest basis or for public interest, an individual can object, and we must stop processing unless we have compelling overriding grounds. For

example, if ACK were sending out fundraising appeals to former students of a church school and someone objects to receiving these, we will cease using their data for that purpose. Additionally, individuals can request that we restrict processing while a dispute is resolved (for instance, if someone contests the accuracy of data or has lodged an objection, we should pause processing that data until the issue is addressed). During restriction, we can store the data but not use it. We will notify the person before lifting any restriction.

9.6 Right to Data Portability:

Under Section 38 of the Act, individuals have the right to obtain and reuse their personal data across different services. Upon request, ACK will provide the individual's personal data in a structured, commonly used, machine-readable format (for example, a CSV or Excel file of their data). They also have the right to request us to transfer their data directly to another data controller or processor, where technically feasible. Data portability primarily applies to data processed by automated means and based on consent or contract. In a church context, this might rarely be invoked, but an example could be a student requesting their academic records be sent from an ACK school to another school, or a scenario where a member moves to a different church denomination and wants a copy of the information they had provided. We will comply with portability requests within 30 days as guided by the Act, provided it does not adversely affect the rights of others.

9.7 Right to Withdraw Consent:

If any processing is based on the individual's consent, they have the right to withdraw that consent at any time. ACK will make it as easy to withdraw consent as it was to give it. For instance, if someone gave consent to be in a church directory, and later changes their mind, we will remove their information from the directory for future editions. Withdrawal of consent will not affect the lawfulness of processing already done, but we will stop the processing going forward. We will inform individuals of this right at the time of obtaining consent.

9.8 Right to Complain and Seek Redress:

ACK will maintain an open channel for data subjects to raise concerns or complaints about how their data is handled. Individuals can lodge a complaint with the designated data protection officer or the responsible office at parish/diocesan level. We will investigate and respond to such complaints in a timely and fair manner. If the individual is not satisfied with ACK's resolution, they have the right to escalate the complaint to the Office of the Data Protection Commissioner (ODPC) or even pursue legal action. Our aim is to address issues internally where possible, through corrective measures or clarification, to maintain trust. We will not retaliate against anyone for exercising their privacy rights.

9.9 Procedures to Exercise Rights:

ACK will develop simple procedures for individuals to exercise these rights. This may include forms or contact emails for making requests (e.g., a dedicated email like privacy@ackenya.org .... for data queries, or a form available at parish offices for access or correction requests). Identity verification will be necessary especially for access, deletion, or portability requests to ensure we are dealing with the genuine data subject or their authorized representative. We will maintain a log of requests and outcomes to demonstrate compliance (accountability). All staff should know how to direct individuals to the proper channel if a request is made (for example, if a schoolteacher is handed a request by a parent to delete data, the teacher should forward it to the school administrator or DPO promptly).

Some limitations or exemptions may apply to data subject rights as per the law (for instance, if honouring a right would infringe on another person's rights, or national security exceptions, etc.), but such cases are expected to be rare in our context. Generally, ACK's posture is to be as accommodating as possible of individual rights, seeing this as part of our pastoral duty of care. Empowering individuals with control over their personal information fosters trust and transparency, consistent with our values.

Data Security and Breach Response

10.1 Chapter Overview

Safeguarding personal data through robust security measures is a cornerstone of this policy. ACK will implement appropriate technical and organizational security measures to ensure confidentiality, integrity, and availability of personal data, and to prevent unauthorized access or disclosure. Additionally, ACK commits to a prompt and effective response in the event of any data breach to minimize harm and fulfill legal obligations. The following outlines our approach to data security and breach management:

10.2 Technical and Organizational Security Measures:

a. *Access Control:*

Access to personal data within ACK will be restricted on a need-to-know basis. Physical records (files, registers) will be kept in secure cabinets or rooms with controlled access. Electronic systems (databases, computers) will be protected by strong passwords or other authentication methods. Each user (staff or clergy) should have unique login credentials, and sharing of accounts is discouraged. Role-based access will be implemented where possible, ensuring individuals can only access the data necessary for their role (for example, an accounts clerk might access payroll data but not health records, a parish volunteer might update membership contacts but not see confidential counselling notes).

b. *Data Encryption and Pseudonymization:*

Where feasible, ACK will use encryption to protect personal data, especially sensitive data, during storage and transmission. For instance, portable devices like laptops or USB drives containing personal data should be encrypted to prevent access if lost or stolen. Emails or electronic file transfers carrying sensitive personal information should be encrypted or password protected. In databases, sensitive fields (like ID numbers or health details) might be encrypted at rest. We will also

consider pseudonymization or coding of data in cases like research or archiving, where data can be processed without direct identifiers once initially collected, thereby reducing risk.

c. *Firewalls and Anti-Malware:*

ACK's IT infrastructure will be secured with up-to-date firewalls, antivirus and anti-malware software. This helps prevent hacking, viruses, ransomware, and other cyber threats that could compromise personal data. Systems will be regularly updated (patch management) to fix security vulnerabilities. Where ACK uses networked systems (such as shared databases across dioceses), professional IT support will be engaged to monitor and protect the network.

d. *Physical Security:*

Offices and storage areas that contain personal data records (e.g., file rooms with parish registers, servers in the IT room, etc.) will have physical security controls. This might include lockable doors and cabinets, biometric access control, alarm systems in offices, visitor sign-in for entry to secure areas, and policies against leaving sensitive documents unattended on desks. For example, baptism and marriage registers, which are sensitive, should be locked when not actively in use. In hospitals, patient files should be kept in secure file rooms or behind staffed stations.

e. *Personnel Practices:*

All persons handling data will be trained on their confidentiality obligations (see 14.0 Compliance and Training). We will implement measures such as confidentiality agreements for staff, rules for clear desk (not leaving papers out), and proper procedures for discarding sensitive documents (like shredding). Employees should report any suspicious activity (like someone trying to gain unauthorized access) to management immediately. Use of personal devices for church work should be governed by policy – e.g., if staff use their own phone or laptop to access church email or data, it should have security safeguards, and any data must be deleted or transferred to church control when they leave their role.

f. Data Protection by Design and Default:

When developing new systems, forms, or processes that involve personal data, ACK will incorporate privacy considerations from the outset. This includes conducting Data Protection Impact Assessments (DPIAs) for new projects with high risk (like deploying a new churchwide database of members or launching a mobile app for a church service). By identifying risks early, we can build in safeguards (for instance, ensuring the app uses secure login and minimal data). By default, we aim to collect and retain only the data absolutely needed and secure it by default settings (e.g., a system might have privacy-friendly default options like not publicly displaying personal data unless opted in).

10.3 Breach Response Plan:

Despite best efforts, incidents may occur. A "personal data breach" is broadly defined as any security incident leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data. ACK has a response plan to manage such incidents:

a. Reporting Internal Incidents:

All ACK personnel must immediately report any suspected or confirmed data breach to the designated authority (typically, the Data Protection Officer or institutional head). This includes incidents like lost or stolen devices/papers containing personal data, external hacking attempts, accidental emailing of data to wrong recipients, or any situation where personal data might have been exposed. Time is of the essence; as soon as an employee or clergy member learns of a breach, they should escalate it. Each ACK institution should know the specific point of contact for reporting (e.g., an ICT officer or the DPO's hotline).

b. Containment and Assessment:

Once reported, the first step is to contain the breach – e.g., disconnect compromised systems from the network, retrieve mis-sent emails, if possible, change access credentials if an account is compromised, etc. The DPO or response

team will then assess the scope and severity of the breach. Key questions: What data was involved (and how sensitive)? How many individuals are affected? Has the breach been stopped or is it ongoing? What are the risks to those individuals – could they face harm such as identity theft, financial loss, reputational damage, physical harm, or other consequences? This risk assessment will guide further actions.

c. *Notification to Regulator:*

If the breach is likely to pose a "real risk of harm" to data subjects, ACK will notify the Office of the Data Protection Commissioner (ODPC) within 72 hours of becoming aware of the breach, as required by law. The notification will include information such as the nature of the breach, categories of data and individuals affected, approximate number of data subjects affected, measures taken or proposed to address the breach, and contact information for ACK's point person. If notification within 72 hours is not possible, reasons for delay will accompany the report. We recognize that ODPC has begun enforcing penalties for breaches, so timely notification is critical to show good faith compliance.

d. *Notification to Affected Individuals:*

When a breach poses a high risk to the rights and freedoms of individuals (e.g., sensitive data exposed, or risk of fraud or harm), ACK will also communicate the breach to the affected data subjects without undue delay. This communication will be done in clear, plain language, advising what happened and what the individual can do to protect themselves (such as changing passwords, monitoring accounts, etc.), and what we are doing to mitigate the harm. Exceptions: if the data was encrypted or otherwise secured such that misuse is unlikely, or if notifying individuals would involve disproportionate effort, we may choose not to inform individuals directly (instead potentially making a public announcement). However, our default is to err on the side of notification when harm is possible, both out of legal duty and pastoral care. For instance, if a laptop with unencrypted parishioner data is stolen, we will likely inform those parishioners so they can be vigilant against any misuse of their info.

e. *Notification between Processors and Controllers:*

If an ACK entity acting as a data processor (e.g., a diocesan office processing data for the province, or an external IT provider) discovers a breach, they must inform the relevant data controller (e.g., Provincial office) immediately and no later than 48 hours of awareness. Our contracts with third-party processors will include an obligation to notify us of incidents promptly (see Chapter 13.0). Internally, the culture should be one of prompt upward reporting.

f. *Investigation and Remediation:*

After immediate containment and notification steps, ACK will conduct a thorough investigation into the cause of the breach. We will document the facts related to the breach, its effects, and the remedial actions taken. The response team will identify any deficiencies in our processes or security that led to the incident and recommend improvements. Remedial actions could include technical fixes (patching a software vulnerability), disciplined training or disciplinary action for staff if it was due to negligence, revising procedures (e.g., encrypting data going forward, or adding an approval step before mass emails), etc. The goal is not only to resolve the current incident but to prevent similar ones in future (continuous improvement).

g. *Record-Keeping:*

ACK will maintain an internal breach register/log of all data breaches, whether they were notifiable to ODPC. This log will record the date, nature of breach, those notified, how it was resolved, and lessons learned. Keeping such records is part of demonstrating accountability and helps in audits or evaluations of our data protection program.

h. *Support for Affected Individuals:*

In line with our pastoral ethos, if a breach occurs that affects our members or others, we will provide appropriate support. For example, if a breach exposed someone to risk of identity theft, we might assist them in contacting authorities or advise on protective steps. If it caused emotional distress (like exposure of sensitive

counselling info), clergy or counsellors should be available to support those persons. Legally, we want to mitigate any damage; morally, we want to help heal any breach of trust.

i. No Concealment:

ACK does not condone concealing breaches. Openness in breach response is key to maintaining trust and complying with the law. Whistleblower protections will be upheld – if any staff reports a security weakness or breach, they will not face adverse consequences for speaking up. The worst scenario is a breach that is hidden or ignored, which often exacerbates harm and liability. Thus, leadership will foster an environment where reporting issues is encouraged.

Data Retention and Disposal

11.1 Chapter overview

ACK will retain personal data only for as long as it is necessary to fulfill the purposes for which it was collected, or as required by law or legitimate organizational interests. Once personal data is no longer needed, we will ensure it is securely disposed of or anonymized to prevent any unauthorized access or use. A thoughtful approach to retention and disposal is essential for legal compliance (avoiding storage of data longer than allowed) and for ethical stewardship (not hoarding personal information indefinitely).

11.2 Establishing Retention Periods:

Each category of personal data processed by ACK will be assigned a defined retention period, considering the purpose of collection and any legal or regulatory requirements. For example:

a. Sacramental and Membership Records:

Records of baptisms, confirmations, marriages, and funerals may be kept permanently or for extremely long periods, as they serve archival and historical purposes for individuals and the Church. However, if such registers are published or made accessible, care will be taken to protect privacy of living individuals (e.g., not publicly disclosing recent entries without consent).

b. General Parish Membership Lists:

If not part of a permanent register, general contact lists should be reviewed periodically (at least every couple of years) to remove those who are no longer active or whose information is outdated, unless there's a reason to keep (such as a person hasn't been seen but hasn't transferred out – the parish may keep for a grace period).

c. *Employee and HR Records:*

Under employment laws, certain records (like contracts, statutory deductions, injury records) must be kept for specified periods (often several years after employment ends). ACK will follow labour law guidelines – e.g., keeping HR files for say 5 years after an employee leaves, then securely disposing or archiving them. Some data (payroll ledgers, pension records) may be kept longer for financial/legal reference.

d. *Student and Academic Records:*

Schools and colleges will establish retention schedules for student records. Transcripts might be kept indefinitely for alumni reference, while disciplinary records might be discarded after a few years post-graduation (unless needed for legal reasons). We will follow Ministry of Education guidelines where applicable.

e. *Medical Records:*

Church hospitals/clinics are often required by health regulations to keep patient records for a minimum period (for adults, possibly 5-7 years after last visit or after patient age of majority for minors, etc.). ACK health institutions will adhere to medical retention laws, then either anonymize or archive old patient files. Sensitive health data that is very old and no longer needed for patient care or legal purposes will be destroyed.

f. *Donor and Financial Records:*

Funding Partner records might be kept for several years for accounting and audit (e.g., 7 years is common for financial records). However, personal data of donors should not be kept beyond that unless needed for ongoing donor relations (with consent).

g. *Email and Correspondence:*

Staff emails or documents that contain personal data should not be stored indefinitely. We will encourage routine archiving or deletion of emails that are no

longer needed. Any emails containing sensitive personal information should be deleted as soon as they are no longer required for the task at hand.

h. CCTV Footage:

If ACK institutions use CCTV for security, the video footage should be retained for a short period (e.g., 30 days) unless it's flagged for investigation of an incident, in which case relevant clips may be retained longer as evidence. Continuous indefinite retention of surveillance footage is not allowed.

11.3 Legal or Consent-Based Extensions:

There are instances where we may keep data longer than the standard period:

a. Required or Authorized by Law:

If a law or regulation mandates a longer retention (for example, certain financial or child protection records may have lengthy retention requirements), ACK will retain data for that period. For instance, if a law requires retaining certain documents for 20 years, that will override a shorter internal schedule.

b. Reasonably Necessary for Lawful Purpose:

The Act allows retention if ***"reasonably necessary for a lawful purpose"***. This could include ongoing litigation (we would keep relevant data until case concludes), or an ongoing investigation, etc. We interpret "lawful purpose" narrowly, to avoid abuse.

c. Data Subject's Consent:

If the individual specifically consents to a longer retention (perhaps for archival contributions or personal reasons), we may retain with consent. For example, an alumnus might allow a school to keep their student work for historical archive. Consent for retention will be documented, and the data subject can withdraw it, in which case we revisit deletion.

d. Historical, Statistical, Research Purposes:

As allowed by law, data may be retained for genuine archiving in public interest, or for scientific/historical research or statistical purposes. In such cases, ACK will ensure appropriate safeguards (like anonymizing data or restricting access) so that the data is not misused. An example: ACK may keep decades of anonymized attendance data to analyse church growth trends.

11.4 Secure Disposal Methods:

When the retention period lapses or data is no longer needed, ACK will dispose of personal data in a secure manner:

a. Paper Records:

Documents containing personal data will be shredded, incinerated, or pulped so that the information cannot be read or reconstructed. If using third-party shredding services, they must be trusted or supervised. Simply throwing papers in the trash or recycling without destruction is prohibited.

b. Electronic Data:

Files will be permanently deleted in a way that prevents recovery. For databases, records will be securely deleted or anonymized in the system. For devices or drives being decommissioned, we will use wiping tools to erase data or physically destroy the storage media if necessary. Simply "deleting" a file (which may still be recoverable) is not sufficient for sensitive data – we aim for secure wipe. Backup copies should also be addressed; when data is deleted from primary systems, we should ensure it is also removed from backups at the next backup cycle or that backups have an expiration.

c. Special Cases:

If data was stored with third-party services (cloud or SaaS providers), we will ensure through contracts that upon termination of service, our data is returned and then deleted from the provider's systems. If individuals requested deletion (right to erasure), we will not only delete active records but also scrub the data from any archives or derivate data sets, unless exempt.

After disposal, a record of what was disposed and when may be kept (this record should not contain the personal data itself, just a log like "Shredded 10 boxes of old HR files for years 2000-2010 on X date"). This can help demonstrate compliance later if needed.

11.5 Suspension of Deletion (Litigation Hold):

In the event of pending litigation, investigation, or audit that involves certain records, ACK may issue a "hold" order to relevant units to suspend routine deletion of related records even if their retention period is over. For example, if a legal dispute arises involving a former student, the school should not delete that student's records even if they are scheduled for deletion. Once the matter is resolved, deletion can resume. Such holds will be decided by senior leadership in consultation with legal counsel.

11.6 Communication to Data Subjects:

Our privacy notices will inform individuals in general terms how long we keep their data (or the criteria used to decide). For instance, a parish registration might say "We will retain your contact information while you are a member of the parish and for up to X years after you cease to be active, unless we are required by law to retain it longer." Transparency about retention helps manage expectations.

Enforcement of sensible retention periods and secure disposal, reduces the risk of data becoming stale and being subject to breaches or misuse. It also aligns with the data minimization principle – not keeping more data than necessary. From a theological perspective, stewardship includes knowing when to let go: just as we don't cling to resources, we no longer need, we should not cling to personal information forever. When its purpose is served, we release it respectfully and securely.

Children's Data Protection

12.1 Introduction:

Children are a vital part of the Church's community and require special protection when it comes to their personal data. In line with our Christian duty to care for the young and vulnerable, and in compliance with legal requirements, ACK has specific provisions for processing personal data of children (individuals under 18 years of age):

12.2 Parental or Guardian Consent:

ACK will not collect or process personal data of a child without the consent of the child's parent or legal guardian, except in exceptional circumstances as permitted by law. For any activity or service directly involving minors – such as Sunday school registration, youth camp forms, school admissions, or health services for minors – we will obtain written consent from the parent/guardian. This consent should cover the specific purposes of processing (e.g., storing the child's emergency contact and medical info for a camp). If online platforms are used (like a diocesan youth website collecting info), age verification and parental consent mechanisms will be implemented. A parent/guardian generally also has the authority to exercise the child's data subject rights on their behalf (see Chapter 9, as also provided in the Act).

12.3 Best Interests of the Child:

Even with consent, ACK will process children's data in ways that are always in the best interests of the child. We adhere to the principle of **"the best interest of the child"** as paramount. This means we consider how any data processing might affect the child's wellbeing, safety, or rights. For instance, when publishing any information or images involving children, we will do so with extreme care – ensuring it does not put them at risk or infringe their dignity. Group photos in a church setting might be used with consent, but we wouldn't publish personal details of children publicly online without a very good reason and consent. If a child's data (say, their

talent or story) is being showcased, pseudonyms or general descriptions might be used instead of full names, unless parents agree otherwise.

12.4 Protective Measures for Children's Data:

Data of minors will be held with heightened security and confidentiality. Staff and volunteers handling children's data (like a Sunday school coordinator with a list of children) must treat it as sensitive. Any online data systems for children (like a school's student information system) should have strong access controls – only teachers, administrators, or parents (for their own children) can access relevant data. When communicating about children, we avoid unnecessary personal details. For example, a prayer list might say "pray for a 10-year-old boy in our Sunday school who is ill" rather than naming the child, unless the family is comfortable with disclosure.

12.5 Data Collected from Children:

ACK will avoid collecting more data from children than necessary. Typically, for ministries, we may need the child's name, age/birthdate (for age group placement), parents' contact, any important health info (allergies, etc.), and perhaps a photo for ID purposes in a secure context. We will not solicit extraneous details about a child's life. Any data collection aimed directly at children (like a VBS form that kids fill in) will be done in a child-friendly manner with simple language, and always with parallel parental oversight.

12.6 Online Services and Social Media:

If any ACK institution offers online services likely to be used by children (for example, a youth ministry app or an e-learning portal in a church school), we will comply with age-related consent requirements. Under 18, a parent should consent for account creation. We will also educate children and parents about not sharing personal info publicly in interactive forums. Our moderators will monitor any online groups for youth to prevent children from posting sensitive personal data publicly. We abide by laws and guidelines on children's online privacy. Moreover, ACK's social media or

website content will not identify children by name alongside photos without explicit parental consent and a clear purpose.

12.7 Photographs and Media of Minors:

Taking and using images or videos of children is a common church activity (Christmas pageants, school events etc.), but it carries privacy risks. ACK will obtain parental permission before photographing or video-recording children for church publications or websites. Even with consent, we will be judicious – for example, we might avoid associating a child's name with their image on a public platform. Recent enforcement in Kenya shows using minors' pictures without parental consent can attract hefty fines, underscoring the importance of this rule. If parents do not want their child's image used, we will respect that fully (perhaps providing alternative activities for the child during photo sessions, etc.). In safeguarding contexts, if a child is under protection or at risk, we will ensure no identifying info or imagery is ever disclosed.

12.8 Child Protection Exception:

There is a narrow exception in the law for cases where obtaining parental consent is not required if one is providing *"child protection services"*. This implies that if ACK (or a related agency) is processing a child's data specifically to protect the child (for example, rescuing a child from abuse or providing social services to a vulnerable minor where contacting the parent might not be in the child's interest), then we may proceed without parental consent. Such cases are likely rare and sensitive. ACK will follow guidance from child protection professionals. Even then, the data would be handled with strict confidentiality and likely in coordination with authorities. This exception will not be misused for general activities – it's meant for cases of protecting the child's life or safety.

12.9 Educating and Empowering Youth:

In our ministry, we also aim to educate young people about their privacy and data protection in an age-appropriate way. For instance, a youth fellowship might have a

session on safe internet use and why the church needs to ask their parents before collecting their info. By building awareness, older children (teenagers) can become active participants in safeguarding their own data, preparing them as they near adulthood to exercise their rights.

Third-Party Processors and Data Sharing

13.1 Introduction:

ACK acknowledges that in carrying out its ministries, there are situations where personal data may be shared with or processed by third parties. This could include service providers, partner organizations, government entities, or other external bodies. Whenever personal data leaves the direct control of ACK, or is handled by someone on ACK's behalf, we will ensure that privacy is still adequately protected. The following rules govern third-party processing and data sharing:

13.2 Due Diligence and Contracts for Processors:

Before engaging any third-party service provider that will handle personal data on ACK's behalf (data processors), we will conduct due diligence to ensure they have the capability and commitment to protect the data. This includes IT providers (for cloud storage, database management, email services), payment processors (for online giving), bulk SMS/email services (for communications), security companies (CCTV or access logs), etc. We will enter into a Data Processing Agreement (DPA) or include data protection clauses in the contract with each processor. Such contracts will stipulate that the processor must only act on ACK's instructions, use the data only for the agreed purpose, keep it confidential, implement adequate security measures, assist ACK in fulfilling data subject rights, and return or delete data after the contract. The contract will also forbid the processor from subcontracting our data to others without permission.

13.3 Sharing with Third-Party Controllers:

Sometimes ACK might share data with third parties who are not simply processors but have their own purpose (data controllers in their own right). For instance, sharing parishioner names with another church for an ecumenical event, or sending student data to a government education authority, or sending beneficiary lists to a donor agency that requires reports. In all such cases, we will ensure there is a lawful basis

(legal requirement, consent, etc.) for the sharing and that it is limited to what is necessary. We will inform individuals through notices or consents when their data might be shared externally and why. If needed, we'll sign Memoranda of Understanding (MoU) outlining each party's responsibilities for data protection.

13.4 No Unauthorized Disclosure:

ACK will not sell or rent personal data to third parties. We also will not disclose personal information to external parties for their own marketing or other independent use without consent. For example, an ACK diocese will not hand over its member list to a commercial Christian bookstore or a political campaign. Even within the church, if data is to be shared between entities (say the province wants to gather all diocesan staff contacts), it will be done with appropriate authorization and purpose, not casually. Any staff or clergy who shares personal data inappropriately (like forwarding a list of congregants to an outside group without approval) will be in breach of this policy and may face discipline.

13.5 Cross-Border Data Transfers:

As noted in Principle 7.9, transferring personal data outside Kenya requires special conditions. If ACK needs to store data on servers abroad (e.g., using a reputable cloud service that hosts in Europe or the US), the DPO will verify that the country has adequate data protection laws or that the service provider offers contractual or other safeguards equivalent to Kenyan requirements. If neither condition can be fully met, we will seek individuals' consent for the transfer of their data abroad (especially for sensitive data), or refrain from such transfer. ACK will also comply with any rules the ODPC issues about approved countries or mechanisms for transfer. For example, if sending staff data to the Anglican Communion Office in London, we might rely on the fact that the UK has strong data protection laws (and perhaps ODPC's recognition of such) or secure a formal agreement. Additionally, when receiving data from overseas (like a partner church giving us their members' contacts for a joint mission), we will treat it with the same care as local data and honour any conditions attached.

13.6 Sharing within ACK Network:

Sometimes data needs to be shared within the ACK family (e.g., a parish informs the diocese of its members, or one diocesan project shares beneficiary info with another diocesan office). While internally this is still within ACK, for privacy it should be treated carefully. We will ensure that internal data sharing is limited to those who need the information and for legitimate purposes. If Diocese A needs assistance from Diocese B and some personal data exchange is required, both must treat that data consistent with this policy. Data should not freely flow within ACK simply because of affiliation; purpose and necessity still govern.

13.7 Third-Party Requests (Government or Legal):

If a third party such as a government agency, court, or law enforcement requests personal data from ACK (for example, a police request for information about a person, or a court order for records), we will verify the legitimacy of the request and ensure there is a lawful basis to comply (usually a legal obligation). We will only disclose what is required by the request and nothing more. Wherever possible, we will inform the affected individual unless the law forbids it. ACK will also maintain a log of such disclosures.

13.8 Joint Activities and Events:

For events or programs run jointly with other organizations (like an ecumenical conference or joint relief project with another church/NGO), personal data might be gathered by multiple parties. In these cases, ACK will clarify who is responsible for what in terms of data protection. Possibly a joint data controller arrangement could be documented. Each participant should agree to protect the data and use it only for the event's purposes. Post-event, the data should not be used by one party for their separate interests without consent (e.g., just because we ran a joint youth camp with Church X doesn't mean Church X can later use the attendee list to advertise their services, unless attendees agreed).

13.9 Public Display of Personal Data:

A special case of data "sharing" is when ACK itself publishes personal data in the public domain (e.g., on notice boards, websites, bulletins). Examples: announcing a wedding or prayer request with names, putting up a list of exam top scorers at a school, or a directory of parish contacts. Before making personal data public, we will consider privacy: we will either obtain consent or at least not divulge more than necessary. Sensitive personal details will never be posted publicly without explicit consent. We will also honour requests from individuals to remove or redact their information from public displays (like opting out of a printed directory). The Christian Daily article referenced earlier highlights that even seemingly innocent publishing of people's images or info by churches requires compliance (like obtaining consent).

13.10 Breach by Third Parties:

In the unfortunate event a third-party processor or partner suffers a data breach involving ACK data, we will treat it as if we had the breach. The third party must inform us immediately, and we will then carry out our breach response (including notifications) per Chapter 10. Contracts will impose this duty on processors. We won't simply say "it was them, not us" – while we will hold the third party accountable contractually, we remain accountable to the individuals and regulator to remedy the situation.

13.11 Auditing and Oversight of Third Parties:

ACK reserves the right to audit or request evidence of compliance from its data processors. For significant contracts, we may periodically review their practices or require them to submit to an independent security audit or certification. If a processor is found to be inadequate in protecting data, we will take remedial action, up to terminating the contract if necessary. The safety of personal data trumps convenience or cost savings from a vendor.

Compliance and Training

14.1 Introduction:

Maintaining compliance with data protection standards is an ongoing process that requires awareness, education, monitoring, and continuous improvement. ACK is committed to fostering a culture of privacy and accountability throughout the church. This chapter outlines how we will ensure that this policy is put into practice and kept effective.

14.2 Training and Awareness:

All clergy, staff, and volunteers who handle personal data will receive training on this Data Protection Policy and relevant privacy practices. New employees and volunteers will be briefed on data protection during orientation. Regular training sessions (at least annually) or refreshers will be conducted to update everyone on best practices, changes in law, or lessons learned from incidents. Training will be tailored to context: e.g., clergy might get guidance on handling pastoral records confidentially; IT staff will get more technical security training; teachers will learn about student privacy, etc. We will also disseminate easy-to-understand guidelines or checklists (for example, “10 Commandments of Data Protection at ACK”) to keep principles fresh in mind. The goal is to make privacy a routine consideration in daily work – just like safeguarding physical safety or financial integrity.

14.3 Leadership Engagement:

Data protection is a leadership issue. The Archbishop, Bishops, Clergy, and heads of institutions are expected to champion compliance. They should lead by example (e.g., following the rules in their own use of data) and encourage their teams to be diligent. Leadership will include data protection status in their reports (for instance, a Diocesan Synod meeting might include an agenda item on compliance, or the Provincial Standing Committee reviews an annual privacy report). By visibly supporting this cause, leaders reinforce its importance.

14.4 Data Protection Officer's Role:

As mentioned in Governance (6.2), the DPO or equivalent has a key role in monitoring compliance. The DPO will conduct or coordinate periodic audits of data processing activities across ACK. These audits will check things like: Are privacy notices being issued? Are consents properly obtained and recorded? Is data kept secure and only accessible to authorized persons? Are records being deleted per schedule? The DPO will also assess new projects or initiatives for privacy risks (Data Protection Impact Assessments) and advise on mitigation. Findings from audits will be reported to management along with recommendations. The DPO acts as an internal watchdog and advisor.

14.5 Compliance Audits and Reviews:

Aside from DPO's audits, ACK may set up internal audit or compliance committees to periodically review adherence to this policy. For example, the Provincial Synod's Standing Committee might request an independent audit (possibly by an external consultant or the internal audit department) of data protection compliance every 2-3 years. Specific areas (like a hospital's patient data system or a diocesan office's records) might be reviewed in depth. The ODPC also has the authority to conduct audits; we will proactively address any areas of weakness before it comes to that. Audit results will be used to update practices and provide further training where gaps are found.

14.6 Documentation and Record-Keeping:

Part of compliance is keeping records that demonstrate what we are doing. ACK will maintain documentation such as records of processing activities (an inventory of key data systems and what data they hold, legal basis, etc.), training attendance records, consent logs, incident logs (for breaches or near-misses), and audit reports. If ACK is required to register with the ODPC due to thresholds, we will ensure that registration is kept up to date. Documentation not only satisfies legal requirements but helps us track our own progress.

14.7 Handling Requests and Complaints:

We will establish efficient procedures to handle data subject requests (as per Chapter 9) and internal/external complaints. Perhaps a dedicated email or portal for privacy requests, with defined responsibility (the DPO or an office) to manage them. We will track response times and ensure we meet the statutory timelines. For complaints, we will have a standard process: acknowledge receipt, investigate, respond with findings and actions, and close the loop. If a complaint reveals a systemic issue (e.g., repeated failure to update records correctly), that should trigger a wider fix.

14.8 Disciplinary Measures:

All ACK personnel are expected to comply with this policy as a condition of their service/employment. Non-compliance may result in disciplinary action in accordance with church canons and HR policies. For instance, if a staff member wilfully breaches confidentiality (like leaking member data) or neglects the security protocols (like sharing passwords or leaving data exposed), they could face consequences up to termination of employment or removal from office, depending on severity. Consistent enforcement of rules is important to show that we take privacy seriously. However, we will also differentiate between malicious/ negligent violations and truly accidental mistakes – the latter we handle more with retraining unless there's clear negligence.

14.9 Continual Improvement:

Data protection is not a one-time task but an evolving practice. ACK will regularly review and update this policy and our procedures considering new laws, technological changes, or incidents that provide learning opportunities. For example, if new regulations are passed (say on data localization or AI use) affecting us, we will incorporate them. If we experience a minor breach that exposed a loophole, we will fix that loophole and improve the system. We might also set new goals each year (like "this year we aim to fully encrypt all laptops" or "we'll implement a new secure church management software with privacy features"). The

policy itself should be formally reviewed at least every two to three years or whenever significant changes in law occur.

14.10 Community and Transparency:

Where appropriate, we will communicate our data protection efforts to our stakeholders. This could mean publishing a summary of this policy on our website or including a note in parish bulletins that "ACK cares about your privacy, for more info contact XYZ." Transparency builds trust: members knowing the church has strong privacy practices will be more willing to engage and share information when needed for ministry. Also, if any significant incident or change happens, we'll be open about it (e.g., if a breach affected many, we might have a brief announcement of what we did to fix it and prevent future issues).

14.11 Regulatory Compliance:

We will stay updated on guidance from the ODPC and ensure timely compliance with any directives, such as filing annual self-assessments or certifications if required in future. If the ODPC issues a corrective action or penalty to any ACK entity, the wider church will treat it as a lesson and implement any necessary changes across the board. Our aim is to never be on the wrong side of the law – not out of fear of fines alone, but because it's right and protects our ability to carry out our mission without interruption or scandal.