

# DATA GOVERNANCE POLICY

## 1. PURPOSE

The purpose of this policy is to establish a structured and secure approach to the collection, management, use, and protection of data across the Kokoda Youth Foundation (KYF). It ensures KYF maintains data integrity, protects personal information, and aligns with relevant legal obligations and internal risk controls. This policy also outlines the roles and responsibilities of staff, volunteers, and third parties, including outsourced IT providers.

## 2. SCOPE

This policy applies to all employees, volunteers, contractors, and third-party partners who access, process, or manage KYF data across all formats (electronic, physical, or cloud-based).

## 3. DATA GOVERNANCE PRINCIPLES

KYF commits to:

**Accountability:** Each user is responsible for handling data ethically and lawfully.

**Transparency:** Stakeholders will be informed of how their data is collected, used, and stored.

**Compliance:** KYF will comply with the Australian Privacy Act 1988 and related laws.

**Security:** All data is to be protected from loss, breach, or unauthorised access.

**Quality:** Data accuracy, completeness, and timeliness must be maintained.

**Ethical Use:** Data must only be used for legitimate KYF operational, reporting, or evaluation purposes.

## 4. DATA COLLECTION

**Personal Information:** Collected only for defined purposes such as registration, communications, health and safety, or evaluation.

**Evaluation Data:** Used to assess program impact, anonymised wherever possible.

**System Tools:** Data collected through platforms (e.g., SharePoint, Power BI, HubSpot, Dynamics) must adhere to this policy and relevant agreements.

## 5. DATA STORAGE AND ACCESS

- Data must be stored on KYF-approved platforms (SharePoint, HubSpot, Power BI, Microsoft Dynamics, etc.).
- Access is role-based and reviewed annually by the CEO or delegate.
- Retention schedules must follow legal requirements and be documented in the Risk Management Register.

## 6. DATA USAGE

- Data is used only for its intended purpose unless legally required or consent is obtained.
- Data may be shared with approved third parties (e.g., BITS Group) under strict confidentiality and data sharing agreements.
- Aggregated, anonymised data may be used for reporting, advocacy, or evaluation.

## 7. DATA SECURITY

- Includes encryption, secure passwords, multi-factor authentication, and offsite/cloud backups managed by IT Service Provider.
- Staff and volunteers must complete regular data protection training and comply with KYF's Crisis Response Policy for data breaches.

## 8. DATA BREACH MANAGEMENT

- All data breaches must be reported immediately and managed as per KYF’s Incident and Emergency Response SOP and Crisis Response Policy.
- Affected individuals and authorities (e.g. OAIC) will be informed if required under the Notifiable Data Breaches scheme.

## 9. ROLES AND RESPONSIBILITIES

**Board of Directors:** Provides oversight for compliance and strategic alignment.

**CEO:** Responsible for implementation and risk escalation.

**Data Governance Committee:** Oversees policy compliance and responds to emerging data risks.

**Outsourced IT:** Manages infrastructure, access controls, security audits, and system maintenance under contractual agreement.

**All Personnel:** Must comply with this policy and report breaches or risks to the People and Processes Manager.

## 10. POLICY REVIEW

This policy will be reviewed annually or earlier if required due to legislative or operational changes. All updates must align with KYF’s Policy Governance and Management Policy and the Policy Development and Approval Procedure.

## 11. COMPLIANCE

Breaches of this policy may result in disciplinary action and, where applicable, legal consequences.

## 12. RELATED DOCUMENTS

This policy aligns with:

- KYF\_GOV\_POLICY\_Risk Appetite Statement\_V1\_2025
- KYF\_GOV\_POLICY\_Risk Management Policy\_V4\_2025
- KYF\_GOV\_POLICY\_Crisis Response\_V1\_2025
- KYF\_GOV\_POLICY\_Child Protection and Risk Management Strategy\_V2\_2025

Related Documents:

- KYF\_GOV\_PROCEDURE\_Risk Management Procedure\_V1\_2025
- BiTS Group IT Service Agreement

## 13. APPROVALS & AUTHORISATION

Version	Approved By	Approval Date	Review Date
1	Board of Directors	9 September	31 October 2026