

Safeguarding Data Storage & Records Management Policy

Policy Statement

The Greyfriars recognise that safeguarding records are among the most sensitive and important categories of information held by the organisation. The proper storage, management, access, retention, and review of safeguarding data are essential to protecting children and adults at risk, supporting lawful and proportionate decision-making, and evidencing effective safeguarding practice.

The organisation is committed to ensuring that all safeguarding information is handled with the highest levels of confidentiality, security, accuracy, and care. All safeguarding records will be created, stored, accessed, and managed within a secure Google Drive/Google Workspace environment, with access strictly limited to those with a legitimate safeguarding role and a clear need to know.

This policy provides the framework through which the organisation will ensure that safeguarding information is:

- securely stored
- accurately and promptly recorded
- accessed only by authorised persons
- shared lawfully and appropriately
- retained in accordance with safeguarding, legal, and regulatory requirements
- available to support governance, audit, case management, and external scrutiny where required

Purpose

The purpose of this policy is to establish a clear, robust system for managing safeguarding records across the organisation.

This policy is intended to:

- protect the confidentiality and integrity of safeguarding information
- ensure that safeguarding concerns, decisions, actions, and outcomes are properly documented
- provide a consistent structure for safeguarding record-keeping across all settings and ministries
- support compliance with data protection law, safeguarding duties, and CSSA expectations
- strengthen governance oversight through reliable, well-maintained safeguarding records
- ensure that the organisation is able to evidence safeguarding practice during audits, reviews, inspections, or case scrutiny

Scope

BVPSkills - Data Storage - Google Drive

This policy applies to all safeguarding-related information created, received, or held by the organisation, whether relating to children, adults at risk, clergy, religious, staff, volunteers, or any person involved in the organisation's life and work.

It includes, but is not limited to:

- safeguarding concern and incident reports
- disclosures, allegations, and complaints
- case management records and chronologies
- risk assessments and risk management plans
- safeguarding meeting notes and decisions
- referrals to statutory or Church safeguarding authorities
- training records and safeguarding matrices
- safer recruitment and vetting records, including DBS/PVG documentation
- safeguarding audits, action plans, and compliance evidence
- policy review records and governance reports relating to safeguarding

This policy applies to all clergy, religious members, trustees, council members, leaders, employees, volunteers, and any other persons involved in safeguarding processes on behalf of the organisation.

CSSA Standards Alignment

This policy supports the organisation's compliance with the Catholic Safeguarding Standards Agency (CSSA) framework, particularly:

- **Standard 2 – Governance and Accountability**
by ensuring safeguarding records are maintained in a way that supports leadership oversight, accountability, and informed decision-making
 - **Standard 3 – Responding Well to Those Who Raise Concerns**
by ensuring concerns are recorded promptly, accurately, and securely
 - **Standard 4 – Care and Support for Victims and Survivors and Those Affected by Abuse**
by ensuring sensitive personal information is handled respectfully, lawfully, and proportionately
 - **Standard 8 – Quality Assurance, Learning and Continuous Improvement**
by ensuring records, action plans, and evidence are accessible for internal review, audit, and safeguarding improvement activity
-

Principles of Safeguarding Data Management

All safeguarding information must be handled in accordance with the following principles:

Accuracy

Records must be factual, clear, timely, and sufficiently detailed. They must distinguish between facts, opinions, allegations, and professional judgment.

Security

Safeguarding data must be protected from unauthorised access, loss, corruption, misuse, or inappropriate disclosure.

Confidentiality

Information must be shared only on a lawful, proportionate, and need-to-know basis.

Accessibility

Safeguarding records must be accessible to authorised safeguarding personnel when needed to support risk management, case decisions, and organisational oversight.

Accountability

Records must support defensible safeguarding decision-making and provide a clear audit trail of actions taken.

Retention

Records must be retained for as long as required by safeguarding, legal, and regulatory obligations and disposed of securely when no longer required.

Consistency

The organisation must maintain a consistent approach to safeguarding documentation, record naming, storage, and review.

Google Drive / Google Workspace Safeguarding Environment

All safeguarding information must be stored in a dedicated, access-restricted Google Drive/Google Workspace safeguarding environment.

This environment may include:

- a dedicated Google Shared Drive for safeguarding
- restricted-access safeguarding folders within Google Drive
- approved safeguarding records maintained in controlled Google Docs, Sheets, and Forms
- private and access-controlled Google Chat spaces where this is appropriate and necessary for safeguarding communication

The safeguarding storage environment must be designed so that confidential records are separated from general operational files and cannot be accessed by those without formal safeguarding authorisation.

Safeguarding records must not be held in informal, unstructured, or unapproved locations.

Security Requirements

The organisation will ensure that appropriate technical and organisational measures are in place to protect safeguarding data.

Access Restrictions

Access to safeguarding records must be limited to:

- the Designated Liaison Person(DLP)
- Deputy DLPs or safeguarding officers, where appointed
- those in leadership who have been formally authorised and have a clear safeguarding-related need to know

Mandatory Controls

The following controls must be in place:

- multi-factor authentication (MFA) is enabled for authorised users
- secure passwords and account protection measures
- restricted folder and file permissions
- external sharing is disabled unless formally approved and demonstrably necessary
- version history enabled where applicable
- audit and activity monitoring, where available
- password protection or encryption for documents where additional protection is needed
- Data Loss Prevention (DLP) measures, where available, to reduce the risk of unauthorised sharing or misuse

Prohibited Storage

Safeguarding information must not be stored:

- on personal devices unless specifically authorised and appropriately secured
 - in personal email accounts
 - on removable media without explicit authorisation and encryption
 - on unapproved third-party platforms or systems
 - in paper files left unsecured or accessible to unauthorised individuals
-

Safeguarding Folder Structure and Records Architecture

The organisation will maintain a clear, logical safeguarding records structure in Google Drive to ensure security, consistency, and audit readiness.

Recommended sections include:

Safeguarding Concerns and Case Files

Restricted folders for:

- individual concern files
- incident reports
- chronologies
- disclosures
- referrals
- case correspondence
- decision logs

Central Safeguarding Register

A live register to provide leadership and safeguarding oversight of core compliance data.

Training Records

Including:

- training attendance logs
- certificates
- refresher dates
- safeguarding training matrix

Safer Recruitment and Vetting

Including:

- DBS/PVG status
- references
- declaration forms
- role risk information where required

Policies, Procedures and Governance

Including:

- current safeguarding policies

- review history
- approval records
- governance papers
- trustee/council safeguarding reports

Risk Assessments

Including:

- ministry or site risk assessments
- event and activity risk assessments
- individual safeguarding risk management plans

Audit and Compliance

Including:

- CSSA evidence
 - safeguarding audits
 - action plans
 - improvement trackers
 - submission materials
-

Recording Safeguarding Concerns

All safeguarding concerns, disclosures, allegations, incidents, and decisions must be recorded as soon as possible after they arise.

Records must:

- use clear, factual, professional language
- include dates, times, names, and locations where relevant
- record the concern in sufficient detail to support understanding and action
- include the immediate action taken
- record the decision of the DLP or the safeguarding lead
- identify referrals made to external agencies or authorities
- record outcomes, follow-up actions, and closure details where applicable

Records must not:

- contain speculative or emotive language
- be altered without a clear justification
- omit significant safeguarding decisions or actions
- be retrospectively rewritten in a way that obscures the original record

Where a correction or clarification is needed, the original record must remain visible through an appropriate audit trail or version history.

Safeguarding Concern Log

The organisation must maintain a standardised safeguarding concern log to support oversight, case tracking, and timely review.

The concern log should include:

- unique reference number
- date and time received
- person raising the concern
- individual(s) involved
- nature of concern
- immediate action taken
- DLP decision and rationale
- referral details
- case status
- outcome
- closure date

This log must be kept securely and reviewed regularly by the DLP.

Central Register

The organisation must maintain an up-to-date Central Register to support leadership assurance and operational oversight.

The register should include, as appropriate:

- names and roles of clergy, religious, staff, and volunteers
- safeguarding responsibilities
- DBS/PVG status and renewal dates
- safeguarding training completion and renewal dates
- ministry/site/location information
- relevant compliance notes or restrictions where appropriate

The register must be:

- accurate and live
- reviewed on a regular basis
- used to identify gaps in compliance
- available to support audit, governance review, and safeguarding planning

Access Control and Confidentiality

Access to full safeguarding records is strictly limited.

Full Access

Full access may only be granted to those with direct safeguarding responsibilities and formal authorisation.

Leadership Access

Trustees, council members, provincial or congregational leaders, or other senior leaders may receive safeguarding summaries, trend reports, risk information, or selected records where necessary for governance, accountability, or decision-making. Such access must remain proportionate and justified.

Review of Permissions

Access permissions must be reviewed regularly and immediately amended when:

- a person changes role
- safeguarding responsibilities cease
- there is concern regarding misuse or confidentiality
- employment, office, or ministry ends

Confidentiality must be maintained at all times. Safeguarding information must never be shared casually, informally, or in any setting that compromises privacy or dignity.

Information Sharing

Safeguarding information may need to be shared with relevant internal or external parties in order to protect individuals and fulfil legal or safeguarding obligations.

This may include:

- statutory safeguarding agencies
- police
- local authority services
- Church safeguarding authorities
- CSSA
- legal advisers
- insurers
- trustees or council members, where oversight duties require it

Any sharing of safeguarding information must be:

- lawful
- necessary
- proportionate
- secure
- recorded where appropriate

Information must be shared only through approved and secure channels.

Data Retention and Secure Disposal

Safeguarding records must be retained in accordance with relevant legislation, safeguarding expectations, insurance requirements, and ecclesial or organisational guidance.

As a general principle:

- safeguarding records must be retained for long-term safeguarding purposes
- records must not be destroyed where there is an ongoing risk, live concern, legal process, or reasonable prospect of future safeguarding relevance
- retention arrangements must be documented and reviewed
- disposal must be secure, authorised, and recorded where appropriate

The organisation should maintain a safeguarding retention schedule or integrate safeguarding requirements into its wider data retention policy.

Data Breach Management

Any actual or suspected breach involving safeguarding data must be treated seriously and reported immediately to the DLP and the person responsible for data protection oversight.

Examples include:

- unauthorised access
- mistaken sharing
- external exposure of files
- loss of records
- compromised accounts
- insecure disposal

All safeguarding-related data breaches must be:

- reported promptly
- risk assessed without delay
- contained where possible
- escalated appropriately

- recorded
- reported to the Information Commissioner's Office (ICO) where legally required

Following any breach, the organisation must review the cause and take action to reduce recurrence.

Monitoring, Quality Assurance and Audit

The organisation will monitor safeguarding record-keeping and data security arrangements to ensure they remain effective and compliant.

This will include periodic review of:

- case recording quality
- timeliness of record completion
- concern log accuracy
- central register completeness
- access permissions
- Google Drive security arrangements
- policy compliance
- audit readiness against CSSA standards

Monitoring findings should inform safeguarding action planning, leadership reports, and continuous improvement.

Roles and Responsibilities

Trustees / Council / Governing Body

Trustees, council members, or the relevant governing body are responsible for:

- ensuring that appropriate safeguarding information governance arrangements are in place
- receiving assurance that safeguarding records are secure, accurate, and maintained appropriately
- supporting policy approval, oversight, and review

Designated Liaison Person (DLP)

The DLP is responsible for:

- ensuring safeguarding records are accurate, timely, and securely maintained
- overseeing case recording and the concern log
- managing appropriate access to safeguarding data
- ensuring that safeguarding information is available to support decisions, referrals, and audits
- reporting safeguarding themes and risks to leadership as appropriate

Deputy DLP / Safeguarding Officers

Deputies or safeguarding officers are responsible for maintaining records in line with this policy and under the direction of the DLP.

IT / Data Protection Support

Those responsible for IT and data protection support are responsible for assisting with:

- access permissions
- MFA and account security
- secure configuration of the Google environment
- breach response support
- technical advice relating to secure storage

17.5 All Staff, Clergy, Religious and Volunteers

All persons involved in safeguarding activity must:

- handle safeguarding information confidentially
 - use only approved systems
 - report concerns promptly
 - avoid retaining unofficial copies of safeguarding records
 - follow this policy and related procedures
-

Related Documents

This policy should be read alongside:

- Safeguarding Policy Statement
 - Safeguarding Concern and Incident Reporting Procedure
 - Case Management / Investigation Protocol
 - Confidentiality and Information Sharing Guidance
 - Data Protection Policy
 - Retention and Disposal Policy
 - Safer Recruitment Policy
 - Risk Management Framework
 - CSSA self-assessment and audit materials
-

Policy Review

This policy will be reviewed annually, or sooner where required by:

- changes in legislation or regulation
 - changes to CSSA standards or expectations
 - significant safeguarding incidents or learning
 - changes to organisational structure or digital systems
-

Appendix A – Required Safeguarding Document Index

The organisation should maintain, as applicable:

Core Safeguarding Records

- safeguarding concern forms
- case files
- incident reports
- chronologies
- decision logs
- referral records
- outcome records

Compliance Records

- central safeguarding register
- safeguarding training matrix
- DBS/PVG records
- safer recruitment documents
- risk assessments

Governance and Improvement Records

- safeguarding policies and procedures
 - review logs
 - audits
 - action plans
 - trustee/council safeguarding reports
 - CSSA evidence documentation
-

Appendix B – Safeguarding Concern Log (Illustrative Fields)

Ref No.	Date Received	Name of Person Raising Concern	Person(s) Involved	Nature of Concern	Immediate Action Taken	DLP Decision / Rationale	Referral Made	Outcome / Status	Date Closed
---------	---------------	--------------------------------	--------------------	-------------------	------------------------	--------------------------	---------------	------------------	-------------

Appendix C – Central Safeguarding Register (Illustrative Fields)

Name	Role	Location / Ministry	Safeguarding Role	DBS/PVG Status	Renewal Date	Training Completed	Refresher Due	Notes
------	------	---------------------	-------------------	----------------	--------------	--------------------	---------------	-------

Appendix D – Google Drive / Google Workspace Safeguarding Controls

Minimum controls should include:

- restricted Google Shared Drive or restricted safeguarding folders
- named user access only
- multi-factor authentication enabled
- external sharing is disabled unless specifically authorised
- password protection or equivalent controls for highly sensitive documents, where appropriate
- routine review of user permissions
- secure file naming and version control
- no use of personal accounts or unauthorised platforms
- DLP or equivalent data handling controls, where available

Document Control

Version	Date	Author	Approved By	Review Date
Ver :1 ,	March 2026	Safeguarding Lead	Trustees	March 2027