Data Management Policy: Metadata

Document Title	CLP-RQ-05: Data Management Policy
Document Type	Policy - A formal statement outlining organisational principles, rules, and expectations that govern decision-making and behaviour
Version	1.0
Approval Date	22nd September 205
Effective Date	22nd September 2025
Review Schedule	Biennial
Next Review Date	21st September 2027
Document Owner (Name, Role, and Email Address)	Polly Needs, Quality and Compliance Manager pneeds@ed.ac.uk
Document Contributors	Polly Needs Mark Lawson Deborah Fry Zoe Lambourne
Target Audience (Select all that apply)	☒ Childlight Staff ☒ Childlight Senior Leadership Team ☐ External Partners & Collaborators ☐ Funders & Sponsors ☐ General Public & Media ☒ Global Data Fellows ☐ Governance & Ethics Committees ☒ Research Teams
Confidentiality Level	Public
Briefing Notes (Any additional information not captured by other fields)	

If you require this document in an alternative format please email Childlight@ed.ac.uk or write to Childlight Global Child Safety Institute, University of Edinburgh, Third Floor, St John's Land, Holyrood Road, Edinburgh, UK, EH8 8AQ.

Childlight Global Child Safety Institute

Childlight Data Management Policy

Data Management Policy

Contents

If you require this document in an alternative format, please email Childlight@ed.ac.uk or write to Childlight Global Child Safety Institute, University of Edinburgh, Third Floor, St John's Land, Holyrood Road, Edinburgh, UK, EH8 8AQ.

1. Purpose and Scope

This policy outlines Childlight's principles and standards for the management of data throughout its lifecycle. It applies to all data collected, created, processed, stored, shared, and archived by or on behalf of Childlight, including data generated through research activities, partnerships, or collaborations. The policy outlines Childlight's parameters for data grading, standards of data security, and processes for data sharing.

This policy applies to all staff, students, partners, and contractors working within Childlight (both research and professional staff) involved in handling data under Childlight's remit.

2. Research Data Management and Childlight's Mission

At Childlight, our mission is to safeguard children across the world from sexual exploitation and abuse. We believe that high-quality, ethically-managed research data is central to achieving this goal. As an institute working to have child sexual exploitation and abuse recognised as a preventable and treatable global health issue, we hold ourselves to the highest standards of research integrity. Good data management – from planning and collection to archiving and sharing – is fundamental to producing trustworthy, actionable evidence. This policy ensures that research data are managed responsibly, securely, and transparently, in alignment with both the values of Childlight and the regulatory obligations of the University of Edinburgh and our partners.

3. Data Management Quality Principles

At Childlight, we define data quality as the degree to which data are accurate, complete, consistent, timely, valid, unique, and fit for the specific purpose they are intended to serve. Data quality is not a one-time achievement but an ongoing commitment essential to research integrity and the trustworthiness of all Childlight outputs.

Childlight's approach to data management is underpinned by the principles of EQIPD, FAIR, and GDPR. Under these structures, we ensure that our data are:

- Transparent and of high integrity: Data are managed in ways that uphold research integrity, documentation, and reproducibility.
- Legal and ethically compliant: All data management activities comply with data protection regulations, including GDPR, DPA 2018, and applicable research ethics standards.
- Aligned with FAIR data principles: We support the creation and curation of data that are Findable, Accessible, Interoperable, and Reusable, where appropriate. With the rise in human reliance on computational support, the FAIR Principles enhance the capacity of a computational system to identify data with minimal human intervention. Further information on FAIR Principles can be found at: FAIR Principles - GO FAIR.
- Secure and protects privacy: Personal and sensitive data are protected through appropriate security, access controls, and governance.
- Collaborative and available: We promote responsible data sharing and reuse to support transparency, innovation, and global child health impact.

4. Data Governance and Ownership

At Childlight, data are core institutional assets that enables evidence-based decision making, impactful research, and effective education. Strong data governance ensures that data are secure, accurate, and responsibly managed throughout its lifecycle – supporting our mission to protect children from sexual exploitation and abuse.

4.1 The Five Safes Approach

Childlight's Data Governance Framework underpins how we manage data to meet legal, contractual, ethical, operational, and strategic obligations. It covers all forms of data – digital or analogue – created, accessed, or used in the course of research or institutional operations. The approach follows a continuous lifecycle of discovery, operationalisation, and sustainment, and is shaped by our institutional values of transparency, integrity, accountability, and safeguarding. All data must be:

- Classified and documented appropriately
- Stored and accessed securely with appropriate controls
- Managed in line with ethical and legal standards
- Used only for legitimate and approved purposes

We adopt the Five Safes Framework to assess and mitigate risks in data use for every Childlight project:

Safe Projects	Is this use of data appropriate?
Safe People	Are the researchers trained and trustworthy?
Safe Data	Have disclosure risks been minimised?
Safe Settings	Are systems and controls adequate?
Safe Outputs	Are results safe to release?

This model ensures proportionate safeguards are in place for all data access, use, and sharing.

4.2 Roles and Responsibilities

Researchers and Project Teams (including Global Data Fellows):	Responsible for familiarising themselves with Childlight's information policies and guidelines and for applying the organisation's data management principles in their daily work. They are expected to follow established processes for the secure use, storage, and sharing of data, and to remain vigilant in identifying and reporting any potential data breaches or security concerns.
Principal Investigators (PIs):	Responsible for ensuring data security and making sure that Data Management Plans (DMPs) and Data Sharing Agreements (DSAs) are in place, maintained, and followed throughout the project lifecycle. They are accountable for compliance with this policy within their research.

Quality & Compliance Manager (QCM):	Provides guidance on data governance and compliance across Childlight. Acting as the primary contact for queries on data compliance, the QCM ensures that best practice and policy updates are communicated effectively throughout the organisation, providing training and support. They also take a lead role in identifying opportunities for the continuous improvement of processes and policies, and are responsible for escalating any data-related risks to the Global Director of Data and the Chief Operating Officer.
Chief Operating Officer (COO):	Supports and oversees data governance activities within Childlight, working closely with the Global Director of Data to ensure data risks are identified, managed, and mitigated effectively.
Global Director of Data (GDD):	Accountable for ensuring that all data processes at Childlight are compliant with relevant policies and regulations. This role also determines the purposes and methods by which data are used within the organisation. Any significant risks relating to data handling are reported by the GDD to the QCM.
IT and Infrastructure Services:	Manage the systems and environments (including Safe Havens and TREs) that support secure data storage, transfer, and access.
University of Edinburgh Chief Information Officer (CIO):	Establishes and maintains the University of Edinburgh's overarching strategy for securing technology and systems. They are responsible for the strategic development and efficient delivery of IT, library, and collections services, encompassing the University's digital strategy, IT provision, teaching and learning technologies, and digital research services.
University of Edinburgh Data Protection Officer (DPO):	Provides Childlight with expert advice on obligations under data protection law and monitors compliance through risk assessments and ongoing oversight. The DPO also acts as the key point of contact on data protection matters for both data subjects and the University CIO.
External Partners and Collaborators:	Expected to adhere to equivalent data management and governance standards as outlined in formal agreements.

4.3 Ownership and Rights

Research data generated by Childlight staff are normally owned by the institution unless otherwise specified in agreements. Rights in data must be documented in Data Management Plans and/or Data Sharing Agreements.

4.4 Personal and Sensitive Data

Personal data refers to any information that can identify a living individual, either directly or indirectly. This includes names, contact details such as email addresses, images, recordings, or coded data where re-identification is possible. Some personal data, such as information on health, ethnicity, or sexual orientation, are classed as special category data and are subject to stricter legal protections.

All processing of personal data must be handled in accordance with data protection law. Where personal or sensitive data are involved, researchers must engage the Quality & Compliance Manager to assess risks and implement appropriate safeguards, such as pseudonymisation or restricted access.

5. Data Lifecycle Management

Childlight adopts a lifecycle-based approach to data management, recognising the distinct needs at each stage:

5.1 Planning

The planning stage is critical to ensuring that research data are managed responsibly and in line with both Childlight's principles and the University of Edinburgh's governance framework. At this stage, all projects must consider the requirements for a Data Management Plan (DMP) and, where personal data are involved, the need for a Data Protection Impact Assessment (DPIA). These measures provide the foundation for lawful, ethical, and secure handling of data across the entire lifecycle of a project.

5.1.1 Data Management Plan

What is a DMP?

A Data Management Plan (DMP) is a formal, living document that outlines how research data will be collected, processed, stored, shared, preserved, and, where appropriate, destroyed, throughout the lifecycle of a project. It ensures that research outputs are managed responsibly, in line with ethical standards, legal requirements, and funder expectations.

When is a DMP required?

All Childlight research projects that involve the collection or use of data are required to produce a DMP at the proposal stage, regardless of whether the data are primary (e.g., surveys or interviews) or secondary (e.g., data obtained from collaborators such as InHope, Child Rescue Coalition, or ONS). Many funders and journals mandate a DMP, and it is also a requirement under Childlight's internal quality framework.

How do we create a DMP?

Childlight researchers should use the University-supported tool DMPonline which provides templates tailored to funder requirements and University of Edinburgh standards. The plan addresses:

1. The nature, expected volume, and source of data being used.
2. Standards, formats, and quality assurance procedures.
3. Data storage and access arrangements, including security measures.
4. Plans for data sharing, publication, and long-term preservation* (including secure disposal).
5. Compliance with legal, contractual, and ethical obligations.

DMPs are reviewed by the QCM at the Project Initiation Document Checkpoint (see Research Project Set-up and Initiation Policy for full details) and by the PI on a regular basis throughout the lifecycle of the project.

How often should a DMP be updated?

Since DMPs are living documents, they must be kept under review. They should be updated whenever there are significant changes in project scope, methodology, collaborators, or data handling arrangements. Updates must be logged and accessible within the project's documentation set.

**Note:* Retention periods must be defined in line with funder, contractual, or disciplinary guidance, but in all cases Childlight applies a minimum retention standard of three years from the completion of the project.

5.1.2 Data Protection Impact Assessment

What is a DPIA?

A Data Protection Impact Assessment (DPIA) is a formal process for identifying and minimising the data protection risks of a project. It systematically evaluates the proposed processing activity (how personal data will be collected, processed, stored, and shared), assessing its scope, context, necessity, proportionality, and compliance with data protection legislation. It identifies potential risks to individuals, evaluates the likelihood and severity of these risks, and documents measures to mitigate them, ensuring that safeguards are built in from the outset.

DPIAs are a core element of the University of Edinburgh's 'privacy by design' approach and a legal requirement under the UK GDPR where processing is likely to pose a high risk to individuals' rights and freedoms.

When do we need a DPIA?

A DPIA must be completed for any research project that involves the collection or processing of personal data, particularly where the data are sensitive, large in scale, involve vulnerable participants (such as children or survivors), or entail novel or high-risk processing methods.

Both the General Data Protection Regulation (GDPR) and the UK Information Commissioner's Office (ICO) dictate project criteria that would require completion of a DPIA. In consideration of these, the University of Edinburgh requires all projects to complete a DPIA where one or more of the following applies:

- The project involves the collection of new information about individuals.
- The project uses information about individuals for a purpose it is not currently used for, or in a way it is not currently used.
- The project involves researchers using new technology that might be perceived as being privacy intrusive.
- The project may result in decisions being made, or actions being taken against individuals in ways that can have a significant impact on them.
- The project involves collection of information about individuals of a kind particularly likely to raise privacy concerns or expectations.
- The project requires researchers to contact individuals in ways that they may find intrusive.

Where there is uncertainty, researchers should consult the University's Data Protection Officer (DPO) who provides advice and oversight, and may escalate assessments where

high residual risks remain. In such cases, consultation with the ICO may be required before the project proceeds.

At what point should the DPIA be started?

The DPIA should be initiated at the earliest stage of project development – ideally alongside the drafting of the Data Management Plan. It must be finalised before any data collection or processing begins. DPIAs are living documents and must be reviewed and updated throughout the project lifecycle whenever changes in methodology, scale, or data sensitivity occur.

How do we carry out a DPIA?

The University provides a standard DPIA template and supporting guidance. The process is designed to be flexible and scalable and a light touch DPIA may be appropriate for low level processing where there is minimal risk.

The process involves:

1. Describing the nature, scope, context, and purposes of the proposed data processing.
2. Assessing the necessity and proportionality of the processing in relation to the project aims.
3. Identifying and evaluating potential risks to individuals' rights and freedoms.
4. Documenting measures to mitigate those risks.

It is the responsibility of project leads to ensure that DPIAs are carried out and maintained for all relevant research. Failure to adequately assess and mitigate risks at this stage may result in project delays, additional costs, or legal non-compliance.

For further information, or to initiate your DPIA, please contact the University's Data Protection Office.

5.2 Collection and Input

Data must be captured using secure, validated systems to ensure accuracy, reliability, and compliance with legal and ethical obligations. Childlight researchers are required to use the Childlight Dataframe Template and Data Grading Process (see section 5.2.2) to promote consistency and enable an initial quality review of all datasets.

5.2.1 Inbound Data

Where data are acquired externally, appropriate due diligence must be completed before any transfer takes place. This includes confirmation of the legal basis for processing, verification of data quality and documentation, and registration of the dataset with the relevant project record.

Data Sharing Agreements

As Childlight frequently works in partnership with external organisations, Data Sharing Agreements (DSAs) form a critical part of safeguarding research integrity. A DSA (or equivalent University of Edinburgh Data Transfer / Access / Use Agreement – see the Childlight Contracts and Collaborations Guidelines) must be in place before data are received or shared. These agreements set out:

- Ownership of the data and rights to reuse or re-share.
- Ethical approvals, contractual limitations, and legal obligations (e.g., under GDPR).
- Security measures to be applied, including encryption, secure storage, and access controls.
- Responsibilities of Childlight researchers and partner organisations in handling, processing, and retaining the data.
- Arrangements for derived data, secondary outputs, and publications.

Childlight researchers must use the prescribed University templates and processes, as described in the Childlight Contracts and Collaborations Guidelines. The Childlight Quality & Compliance Manager must also be informed of all inbound or outbound transfers.

Receiving Data (Inbound Data Sharing)

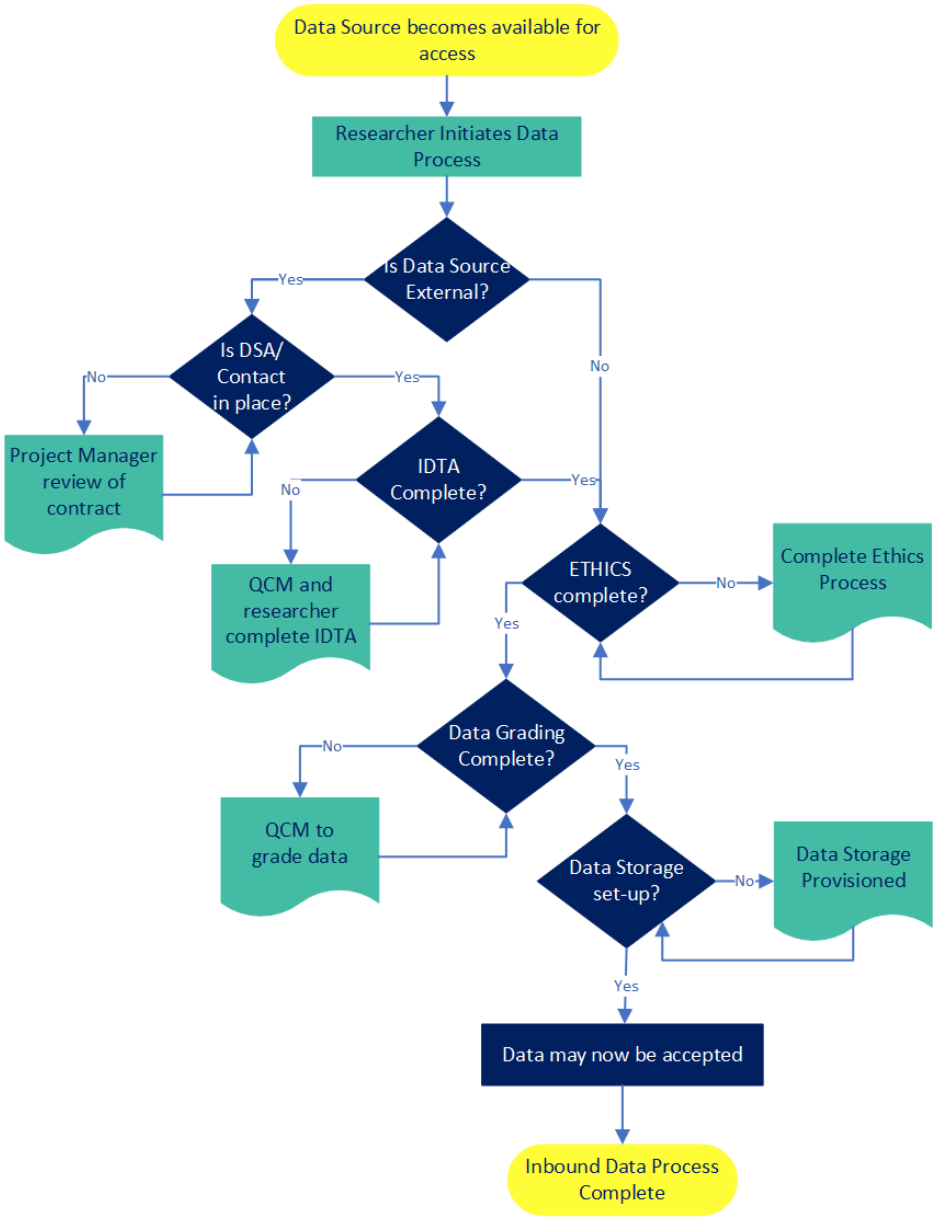
When receiving data from a partner organisation or external provider, the following steps must be followed:

1. Confirm permissions and approvals – establish the legal basis for processing, verify that necessary ethical approvals (e.g., REC approval, DPIA) are in place, and ensure a signed DSA has been completed.
2. Verify data quality and documentation – review metadata, provenance, grading, and completeness before incorporating the dataset into Childlight's research processes.
3. Register the data – record the dataset within the relevant research project record, ensuring traceability and linkage to approvals.

4. Pre-arrange storage – ensure secure storage within an approved University of Edinburgh environment (e.g., DataStore, DataVault, SafeHaven) is in place before data transfer.
   Due diligence – complete the Childlight DSA checklist (see Appendix 1) and, where applicable, the University of Edinburgh Incoming Data Transfer/Access/Use Agreement form

Researchers must not accept data unless *all of the above requirements* are met. Data may not be stored in personal locations, consumer-grade cloud storage, or unapproved devices. Any concerns or uncertainties should be escalated to the Quality & Compliance Manager before acceptance.

Figure 1: Inbound Data Process



DSA – Data Sharing Agreement
IDTA – Inbound Data Transfer Agreement
QCM – Quality and Compliance Manager

5.2.2 Data Grading

As a research institute working in sensitive domains, Childlight must apply clear and consistent processes to assess and manage the data it handles. All research data, whether generated internally or provided by external partners, must be graded appropriately to ensure compliance with legal, ethical, and institutional standards, and to inform where and how it may be stored.

Types of Data Handled

Childlight typically works with two broad categories of data:

- Internally generated data, such as:
  - Participant interviews
  - Aggregated open-source datasets
  - Literature, scoping, or systematic review data
- Externally provided data, including:
  - Administrative data (e.g., health, education, social care)
  - Primary captured data (e.g., survey responses)
  - Machine-captured data (e.g., biometric inputs, telemetry)

The source of the data (internal vs. external) is less important than the nature of its content when determining how it should be managed.

Determining Data Grade

All data handled by Childlight must be assessed based on three core questions:

1. Does it contain personal information (PII)?
2. Does it contain sensitive content?
3. Is it legally and ethically permissible to store this data?

If the answer to any of these indicates elevated risk, the data are likely to require stronger safeguards and must be classified accordingly.

Note: In Childlight's data context, "risk" can mean:

1. Risk of personal identification
2. Risk of direct or vicarious trauma
3. Risk of contractual contravention
4. Risk of reputation (upon data breach or security issue)

Personal Information

Personal Identifiable Information (PII) refers to data that can (or can be perceived to) identify a specific individual. This includes names, dates of birth, national IDs, addresses, or any unique identifiers. In most cases, Childlight's research does not retain PII. Where personal data is involved:

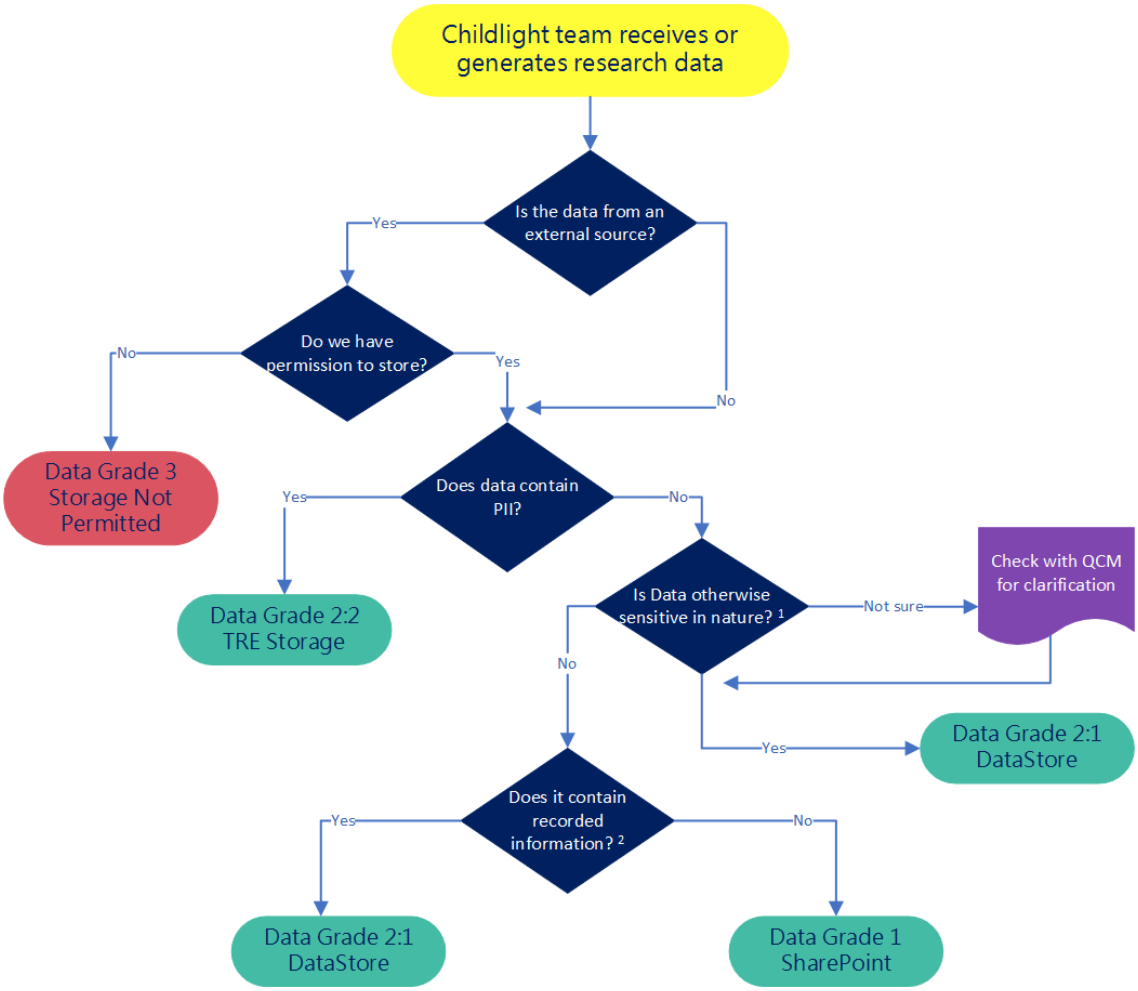
- The research project must have specific ethical approval.
- Informed consent must explicitly permit data retention.
- A Data Protection Impact Assessment (DPIA) is required.

Where permitted, personal data are classified as Grade 2:2 and must be stored within a Trusted Research Environment (TRE).

Sensitive Content

Data may be deemed sensitive if it includes descriptions of illegal activity; experiences or disclosures from victims, survivors, or professionals; or, content that could cause direct or vicarious trauma. Even where PII is not present, this type of material requires heightened security and is classified as Grade 2:1.

Figure 2: Data Grading Process



[1] E.g., Graphic descriptions or filenames of sexual/illegal activities which some researchers/staff may find traumatic
[2] E.g., If participants have been recorded on Teams, video or audio interviews/meetings

Permission to store - this alludes to contracts for data to be permitted to be stored and ethical approval of project data to be stored and data are legal to store in UoE/UK
PII – Personally Identifiable Information - names, addresses, identifiers etc
TRE – Trusted Research Environment aka Data Safe Haven
QCM – Quality and Compliance Manager

The Childlight Data Grading System

Childlight uses a three-level data grading system to determine the level of protection and storage required:

Grade 1 – Low Risk
These datasets pose minimal risk. They do not include PII, sensitive content, or legal/contractual restrictions. Examples: • Aggregated datasets from open sources • Summary statistics or public data • Internal planning documents Permitted storage: SharePoint, OneDrive (as a temporary measure only).

Grade 2 – Moderate to High Risk
Grade 2 data are subdivided: • Grade 2:1 – Contains sensitive but non-identifiable data. This might include distressing content or case material without names. Permitted storage: University of Edinburgh DataStore • Grade 2:2 – Contains identifiable or special category personal data. Must have explicit ethical approval and a DPIA. Permitted storage: Trusted Research Environment (TRE)/Safe Haven

Grade 3 - Prohibited
Grade 3 refers to data that must never be stored or handled by Childlight. This includes illegal material such as Child Sexual Abuse Material (CSAM), which is prohibited under UK law. If any member of staff receives, is sent, or inadvertently encounters CSAM: • Do not open, save, or share the file • Notify your line manager and the Quality and Compliance immediately

Possession of such material is a criminal offence, and any incident may place both you and Childlight under investigation by both the university and law enforcement in Scotland.

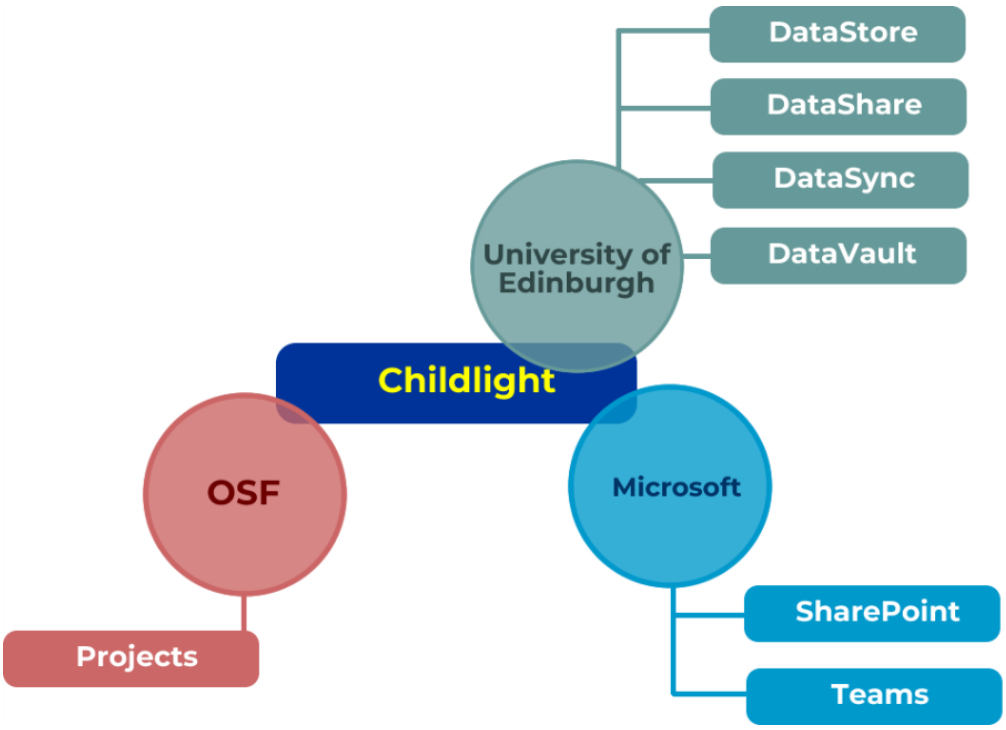
5.3 Data Storage

Childlight applies a tiered approach to data storage, ensuring that each dataset is handled in a manner proportionate to its sensitivity as determined by data grading (see Section X: Data Grading). All data storage locations must:

- Be access-controlled, with permissions reviewed regularly.
- Support audit trails or logging where required.
- Be included in the project's Data Management Plan (DMP).
- Comply with Childlight's IT and Information Security standards.

The appropriate storage solution must be selected during project setup and reviewed regularly to reflect any changes in data classification, sensitivity, or partnership arrangements. The schematic below indicates the scope of the different data storage mechanisms of the platforms in use at Childlight.

Figure 3: Childlight Data Storage Platforms



5.3.1 SharePoint

Permitted Data Grade: Grade 1 (Low Sensitivity)

SharePoint, hosted within Childlight's Microsoft 365 environment, is the default location for storing non-sensitive data. It is best suited for administrative files, general project documentation, and low-risk research materials that do not contain identifiable or confidential information.

This platform supports collaborative work through shared team sites and version control, and access is restricted to authorised users via institutional login credentials. The Quality and Compliance Manager reviews permissions regularly to ensure appropriate access. All data are backed up automatically within Microsoft's secure cloud infrastructure.

SharePoint must not be used to store personal identifiers, special category data, or any information classified as confidential or sensitive.

5.3.2 DataStore

Permitted Data Grade: Grade 2:1 (Moderate Sensitivity)

DataStore is a secure file storage platform managed by the University of Edinburgh. It is designed to support research data that requires additional protection, including content containing personal identifiers, pseudonymised information, or confidential project data.

Access to DataStore is granted via institutional credentials and permissions are managed at the organisational level. When used for collaborative projects, access controls must be clearly defined and documented, with oversight maintained by the relevant data controller or project lead. DataStore is only available when on the University premises or connected through an authorised VPN account to the University network – sharing to non-University staff is not possible.

While DataStore provides robust protection for moderately sensitive data, it is not suitable for datasets requiring a controlled research environment. Projects involving high-sensitivity data must instead use a Trusted Research Environment or Safe Haven.

5.3.3 Trusted Research Environment (TRE) / Safe Haven

Permitted Data Grade: Grade 2:2 (High Sensitivity)

High-risk or regulated datasets must be stored and processed within a Trusted Research Environment (TRE), also referred to as a Safe Haven. These are secure computing environments that allow approved researchers to access sensitive data (e.g., identifiable health data, unconsented personal data) under strictly controlled conditions.

Childlight makes use of the Safe Haven operated by the Edinburgh Parallel Computing Centre (EPCC), which meets the standards set out in the Five Safes Framework, the Scottish Government Charter for Safe Havens, and the UK Health Data Research Alliance (HDR UK) principles. This ensures that sensitive data are handled in line with national governance requirements and public expectations for ethical use.

Key safeguards are embedded across the system include:

- Access control: Role-based access and multi-factor authentication
- Data encryption: At rest and during transmission
- Audit and monitoring: Continuous logging and analysis of user activity
- Incident response: Predefined procedures for handling data breaches
- Public involvement: Increasing integration of public voices in data use decisions

The Five Safes is a risk management framework that underpins all TRE operations:

- Safe People: Only appropriately trained and accredited researchers may access data. Admin and user access is strictly role-based.
- Safe Projects: Only approved research projects that meet ethical, legal, and contractual requirements may use the data.
- Safe Settings: Secure, access-controlled environments (like EPCC's Safe Havens) where data are protected from download, copying, or unauthorised access.
- Safe Data: Data are minimised, anonymised, or pseudonymised as appropriate. Access is limited to what is required.
- Safe Outputs: Research outputs are screened before being exported. No identifiable data may leave the secure environment.

Operational oversight is shared between the infrastructure provider (EPCC), who is responsible for the technical environment, and governance teams (eDRIS), who approve projects, monitor compliance, and ensure ethical standards are upheld.

Use of the Safe Haven is mandatory for Childlight projects involving sensitive health, social, or administrative datasets, particularly where legal or contractual requirements specify a controlled environment. Any proposed use must be discussed with the Quality and Compliance Manager at the planning stage, included in the Data Management Plan, and supported by a Data Protection Impact Assessment (DPIA) where personal data are involved. No data may leave the TRE unless it has been appropriately screened and authorised.

5.3.4 Disallowed Storage: OneDrive

While OneDrive is available as part of the Microsoft 365 suite, it is not an approved location for research data storage. Unlike SharePoint, OneDrive is tied to individual user accounts, which are automatically deleted upon account deactivation (e.g., when staff leave). This presents risks to data integrity, continuity, and auditability. OneDrive may be used temporarily for file transit (e.g., for draft documents), but it must not be used as a primary or long-term storage solution.

Note: There is no approved storage location for Grade 3 data. Data classified as Grade 3 poses a significant legal or ethical risk and must not be stored on any system. This includes data for which Childlight does not have lawful basis, appropriate consent, or contractual permissions to retain. If a Childlight member of staff is in possession of Grade 3 data they should immediately notify the Quality & Compliance Manager.

5.3.5 Other Storage Locations

The below storage options are utilised at the point of sharing data externally. More information can be found in section 5.5 Data Sharing.

DataShare	DataShare is the digital repository of research data and is typically associated with data which accompanies an existing or forthcoming publication. A deposit by University research staff may be made into the DataShare service, thereafter a persistent identifier (DOI) will be issued for external researchers to access the data.
DataSync	DataSync is a university service which allows files up to 20GB in size to be shared with anyone, internal or external to the University and may be accessed using the web application. It is akin to DropBox, and is typically used during the research phase of a project.

DataVault	DataVault is a long-term storage facility within the University where research data may be stored following the conclusion of a research project.
Open Science Framework	Childlight supports an Open Science approach to research and uses the Open Science Framework (OSF) as a platform for collaboration with global partners. OSF provides a secure and flexible environment for storing project files, sharing data, and coordinating work across institutions. Researchers can make use of private workspaces during active project development, with the option to transition materials into publicly accessible, publishable outputs. This supports transparency, reproducibility, and effective collaboration from project conception through to final research dissemination.

5.4 Processing and Analysis

Data processing and analysis are core stages in the research lifecycle and must be carried out in a way that protects research integrity, ensures compliance with data protection legislation, and maintains the trust of Childlight's partners and participants. While the specific analytical methods will vary depending on the project, the following standards apply to all processing and analysis activities:

Access Control	Only authorised individuals with a legitimate research need may process or analyse research data. Access permissions must be reviewed regularly and withdrawn promptly when no longer required. Sensitive datasets should only be accessed within secure University of Edinburgh environments or trusted external safe havens, and never on unapproved devices or personal cloud services.
Documentation and Auditability	All processing of personal or sensitive data must be appropriately documented. This includes recording the nature and purpose of the processing, the individuals involved, and any transformations applied to the dataset. Documentation should be maintained within the project's Data Management Plan (DMP) and, where applicable, in compliance records such as Data

	Protection Impact Assessments (DPIAs). This ensures that analyses are transparent, reproducible, and auditable.
Secure Processing Environments	Processing must be undertaken within secure, validated environments that are proportionate to the sensitivity of the data. Examples include the Office for National Statistics (ONS) Secure Research Service or other University-managed Trusted Research Environments (TREs). Researchers must not download or process sensitive datasets outside these approved systems.
Quality and Compliance Oversight	Researchers are responsible for ensuring that data processing adheres to approved project protocols and ethical review requirements. Any deviation must be documented and, where necessary, approved by the relevant governance body. Data minimisation principles should be applied throughout processing and analysis, ensuring that only the data necessary for the stated research purpose are used.

5.5 Data Sharing

Childlight endorses the UKRI and international best practice view that data sharing benefits the public by fostering collaboration, innovation, and transparency. Research data should be handled in line with the FAIR principles and managed in accordance with related initiatives such as DORA (Declaration on Research Assessment), ORCID (Open Researcher and Contributor ID), digital object identifiers (DOIs), and use of standard open licences for sharing research data and code.

Please see section 5.2.1 for information around Data Sharing Agreements.

5.5.1 Purpose and Principles of Data Sharing

Childlight is committed to responsible, secure, and impactful data sharing that enables transparency, reproducibility, collaboration, and the advancement of research in line with FAIR principles:

Findability	Research data should be readily discoverable by both humans and machines. This is achieved through the use of clear, comprehensive metadata that accurately describes the dataset's content, context, and origin. Metadata should include relevant

	keywords and follow established standards to support indexing in institutional or discipline-specific repositories.
Accessibility	The conditions under which data can be accessed must be explicitly stated. Whether data are openly available under a standard licence (e.g., CC-BY) or require restricted access through a formal request or agreement, the access procedure must be transparent and well-documented. All datasets should be stored in systems that support long-term access and retrieval.
Interoperability	To facilitate integration with other datasets and workflows, data should be formatted using open, non-proprietary standards and documented using controlled vocabularies where possible. File types should be widely supported within the relevant research community, and metadata should align with recognised schemas to ensure compatibility across platforms.
Re-Use	Data should be sufficiently well-described and documented to enable future reuse by researchers beyond the original project team. This includes providing information on the dataset's provenance, methodology, limitations, and conditions of use. Licensing information must be clearly stated to define how the data can be reused, and appropriate citation formats should be provided to support acknowledgement and attribution.

While the FAIR principles provide the foundation for effective and sustainable data sharing, Childlight also recognises the importance of additional principles that ensure data sharing is conducted ethically, legally, and responsibly. These include:

- Compliance with ethical, legal, and contractual obligations
- Risk-based assessment of sharing practices
- Maximising research impact through openness wherever possible
- Ensuring data quality and integrity before sharing
- Clear documentation of access rights, terms of use, and retention periods

These considerations ensure that data sharing is not only technically sound and discoverable but also aligned with Childlight's values, research governance frameworks, and societal expectations.

Childlight endorses the UKRI view that sharing research data comes with significant benefit to the public. Sharing data encourages innovation and scientific scrutiny; fosters collaboration and avoids unnecessary duplication; enhances research visibility, citation,

and impact; enables secondary analysis, education, and training; and, aligns with funder and journal requirements.

5.5.2 Preparing Data for Sharing

Before sharing data:

- Ensure the dataset is finalised, cleaned, and documented;
- Organise files with consistent naming conventions and folder structures;
- Conduct quality control checks (e.g., calibration, standardised data collection protocols);
- Ensure data are appropriately anonymised or pseudonymised; and most importantly,
- Check for written confirmation of data grading level, data storage means, data transfer process and route, and contract terms and clauses – including limitations and specific provisions, where relevant. These data sharing terms will typically be outlines in the Data Transfer Agreement (DTA), Memorandum of Understanding (MoU), or in the overall contract/agreement with the third-party organisation.

5.5.3 Internal Data Sharing

Internal sharing should occur through secure, managed platforms. These include SharePoint and DataStore.

As described in section 5.3.1, SharePoint is the primary location for storing and sharing Grade 1 research data and documentation. All team members are given access during induction and the Quality and Compliance Manager oversees team-based permissions to control editing and visibility. Team members may grant access to internal colleagues via “share” or “copy link” for specific files or folders. Links that have been copied can be sent over Teams or in emails. It is inadvisable to download documents to send them as email attachments – such duplication lowers the integrity of version control and risks individuals accessing outdated documentation.

DataStore, used for Grade 2:1 data, can only be accessed via VPN or directly under the internal university network. Project folders on DataStore are secure and limited to specific research teams for shared access to sensitive datasets.

It is best practice to maintain clear folder hierarchies and naming conventions on both SharePoint and DataStore to enable effective intra-team access to shared documents. Further information can be found in the Childlight Document Management Policy.

5.5.4 External Data Sharing

Childlight is a global data institute and works with many partners across a large and diverse network of partners. There are often scenarios where data needs to be handled from partners as well as being shared out. The data sharing may also be facilitated as part of the publication process (FAIR policy) and correct authorised channels should be engaged with for this sharing process.

External sharing is only permitted if:

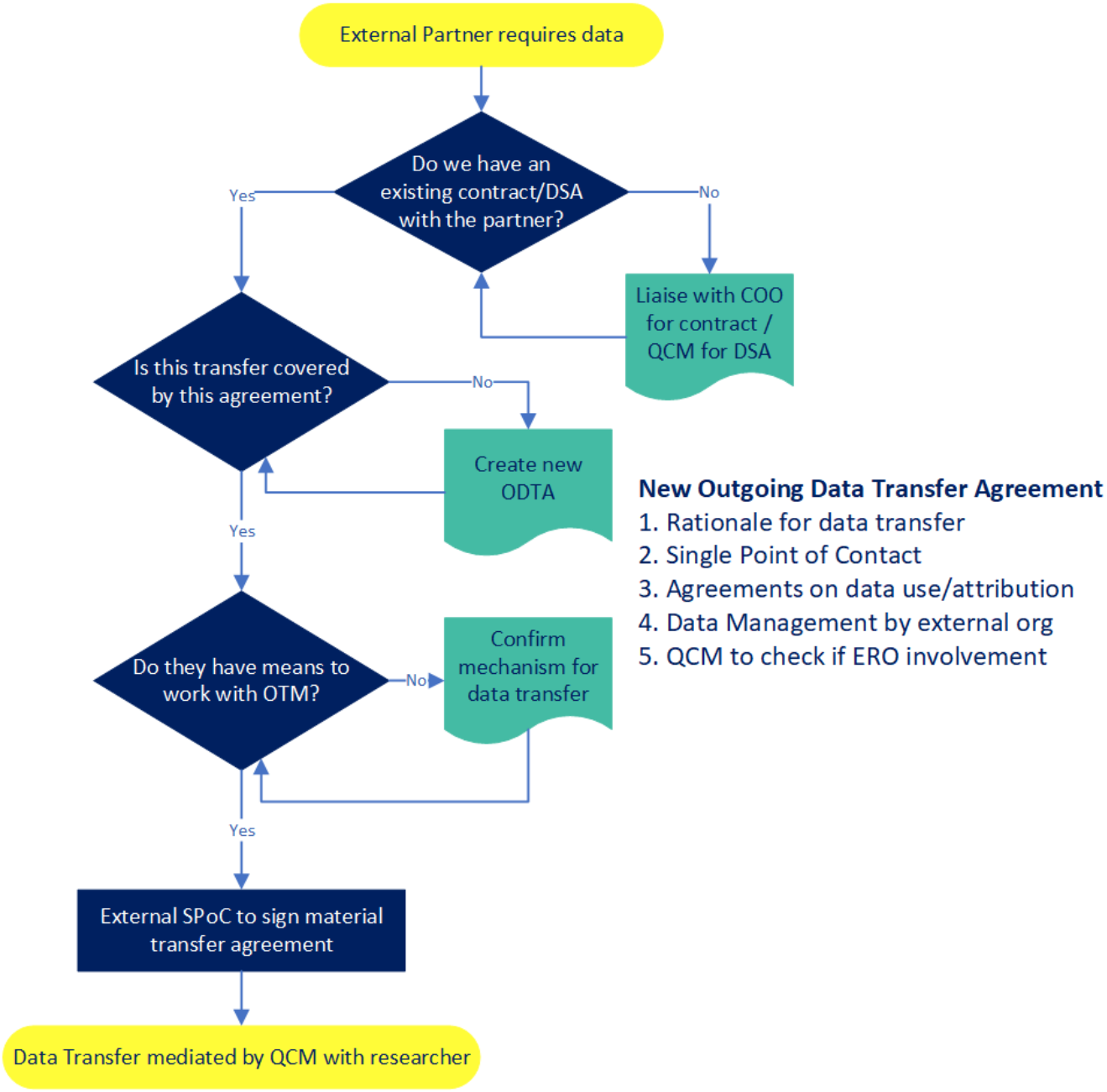
- A Data Sharing Agreement (DSA) or Memorandum of Understanding (MoU) is in place
- Risks are documented via DPIA and approved by the Global Director of Data
- The data being shared complies with contractual, ethical, and legal conditions
- All internal checks and approvals are complete.

5.5.5 Sharing Platforms Hierarchy

Open Science Framework (OSF)
Primary workspace for sharing Grade 1 datasets – facilitated by contributor access to the shared project workspace. This portal provides a secure and globally accessible platform for data collaboration utilising the underlying concepts for Open Science.
DataSync
University-supported alternative to email for secure one-off file sharing. DataSync is a drop-box style service that is both supported and approved by the University of Edinburgh. It protects data by only sending a link to the DataSync file, which is emailed to the recipient can and only be accessed from that specific email account. Further information can be found on the University of Edinburgh's DataSync pages.
DataShare
Edinburgh DataShare is an online digital repository of multi-disciplinary research datasets produced at the University of Edinburgh. It allows researchers to publicly upload, deposit, share and license data for online discovery and reuse. Used only

post-publication, the uploads are made available through Digital Object Identifiers (DOIs). Further information can be found on the University of Edinburgh's DataShare pages.
Email
Emailing research data should be avoided unless all of following criteria are met: • There is no risk to the data should there be a breach or security compromise • The person being emailed is the correct recipient of the data • The email address is an authentic email address and not a free service style email account (e.g., Gmail, BT, Hotmail, AOL etc) • The transport of the data is permitted by email • All other safeguards are in place to ensure the data is protected (i.e. zip archive with a password)

Figure 4: Outgoing Data Processes



OTM – Outgoing transfer method (the means of getting data to the external organisation/partner
SPoC – Single point of contact - must be a named and approved/authorised member of external organisation on DSA/Contract
ODTA – Ongoing Data Transfer Agreement - document created by ERO for authorisation of data transfer

5.6 Data Retirement

At the end of a project's active phase, Childlight applies a clear and compliant strategy for data retirement. This includes defining retention periods, secure archiving, and appropriate disposal in line with legal, ethical, and institutional requirements.

5.6.1 Retention Periods

Retention addresses the question of how long data should be kept. Childlight follows the University of Edinburgh's Research Data Management Policy, which sets a minimum retention period of three years from the end of a project. However, longer periods may be required to meet funder, contractual, or disciplinary obligations. All Data Management Plans (DMPs) must specify retention schedules, taking into account these influences and ensuring transparency and accountability.

In accordance with the UoE Data Protection Policy, UK GDPR laws, and good research practice, researchers must avoid retaining personal data beyond what is necessary to fulfil research obligations or regulatory requirements.

5.6.2 Archiving and Disposal

Data with enduring research, scholarly, or institutional value should be preserved for the long term. Archiving at Childlight follows established best practices to ensure the continued integrity, provenance, and usability of data. Recognised digital archiving standards must be used, and where appropriate, legacy or high-value records may be transferred to the Edinburgh University Archives. Please see the Research Project Closure guidelines for further information on retention.

Equally important is the secure disposal of data that no longer require retention. In line with the university's retention schedules and Childlight's internal procedures, unnecessary data must be destroyed in a safe and responsible manner. For electronic records, this means permanent deletion within systems, including backup or local storage, using secure wiping tools or with IT Services support. For paper or other sensitive physical materials, confidential shredding or authorised University recycling services must be used.

All disposal actions must be fully documented, including the dataset or record concerned, the method of destruction, the date, and the authorisation. This ensures a traceable audit trail and demonstrates compliance with both institutional and data protection requirements.

6. Data Security

Data security is essential to safeguarding research integrity, individual privacy, and organisational trust. At Childlight, this means protecting digital information against unauthorised access, corruption, or loss across its entire lifecycle.

Childlight applies a layered, risk-based approach, aligned with the University of Edinburgh's Information Security policies and sector best practice. Core safeguards include encryption, role-based access controls, and user management to ensure only authorised individuals can access sensitive information. As described in this policy, all data are processed and stored within secure University of Edinburgh environments, with regular audits and monitoring to protect integrity.

Staff, students, and affiliates must follow incident reporting procedures in the event of any suspected breach. Security measures are applied proportionately to the level of data sensitivity, and protections extend to all contexts where Childlight data are accessed – whether on university premises, at home, or while travelling.

6.1 Data Breach

A data breach occurs when personal, sensitive, or confidential data are lost, accessed, disclosed, or otherwise compromised by unauthorised individuals. Breaches may result from cyberattacks, theft or loss of devices, insider misuse, or human error (e.g., sending data to the wrong recipient).

Data breaches can have serious financial, reputational, legal, and operational consequences, and may undermine trust in both Childlight and the University of Edinburgh. In accordance with the General Data Protection Regulations (GDPR) 2016, the university has obligations including notifying the Information Commissioner's Office (ICO) of any security breach within 72 hours of being made aware of the breach.

Detecting and Reporting a Data Breach

If a data breach is suspected or confirmed, staff must:

1. Immediately notify the Childlight Global Director of Data and the Childlight Chief Operating Officer.
2. Inform their line manager or PI (if the breach relates to a research project).
3. Record details in writing, including what happened, when it occurred, the type of data involved, and who may be affected, using the Data Breach Reporting Form at Appendix 2.
4. Follow the University of Edinburgh Data Breach Procedure if the incident occurs out of hours.
5. Notify the Quality and Compliance Manager who logs the incident in the Childlight Data Breach Register to support oversight, learning, and reporting.

Receiving Data in Error (being the recipient of a data breach)

There may be occasions where data is inadvertently or mistakenly shared by a third-party to a Childlight staff member. If this happens, the individual must:

a. Not open, forward, save, or process the file (as this may make the Childlight individual complicit in the data breach).
b. Notify the Childlight Global Director of Data and Childlight Chief Operating Officer.
c. Document in writing the incident and actions taken by completing the Data Breach Reporting Form (see Appendix 2), which should then be submitted to the Quality and Compliance Manager for inclusion in the Data Breach Register. This will capture:
    - When you became aware of the receipt of the data
    - The nature of the data impacted by the breach
    - Who may be impacted by the breach
    - What actions you have taken within Childlight
    - Anything else you have actioned
d. The above can be directly entered into the Seek advice on whether to notify the University of Edinburgh Data Protection Officer (DPO). If you should need to contact the UoE DPO (dpo@ed.ac.uk) include in your report the details as noted in point ‘c’.
e. Send a new email to the sender confirming receipt in error and advise them to escalate internally to their own DPO team.
f. Delete the email and do not save any of the attached, enclosed or linked data.

All staff will receive training on recognising and responding to data breaches, including simulated “phishing” exercises to improve readiness.

6.2 Device Security

University-managed laptops are provided to Childlight staff. These devices are subject to the University's information security standards and remote management policies.

Note: Students and Global Data Fellows use their own devices to carry out their work, and should ensure that their devices are able to meet the expectations set out throughout this policy, including the use of a Virtual Private Network (VPN) where appropriate.

Portable devices (including laptops, tablets, smartphones, and removable media) carry heightened risk of loss, theft, or interception, especially when taken abroad. The disclosure of data stored on a lost or stolen device is typically more serious than the physical loss of the asset itself.

Core Device Security Measures

- Devices used for Childlight work must use full-disk encryption in line with university standards.
- Personal devices should not hold university data unless explicitly approved, and only if encrypted.
- Devices must be kept secure at all times (e.g., in a locked room, cabinet, or locker when unattended).
- Devices must have automatic locking enabled after periods of inactivity.
- Passwords must never be written down or stored with the device.
- University-supplied devices should be used primarily for work purposes to minimise the risk of malware.
- Loss or theft of any device (University or personal) must be reported immediately to:
    - Childlight Quality & Compliance Manager
    - Line Manager
    - College Information Security Team
- Staff must apply all University security updates and patches promptly (these are normally applied automatically to managed devices).

Other Security Measures

Further actions employed by Childlight staff to reduce risks to data security and protect sensitive data:

- Two-factor authentication (2FA) must be enabled for all accounts used to access Childlight or University systems.

- Use of University of Edinburgh VPN (Virtual Private Network) when working off-site or remotely from home.
- Firewall and anti-virus protection installed on all computers.
- Controlled access to research data files through password protection or encryption
- Identification and use of appropriate storage
- Controlled access to rooms and equipment where data (digital or physical) are held
- Ensuring data providers' conditions of consent are met
- Anonymisation techniques or data aggregation to avoid disclosure of sensitive data
- Never storing highly sensitive data on cloud services, including Google Drive, or on machines connected to an external network
- Using approved data sharing services for transferring data to external partners or team members
- Using approved devices for data transfer

Removable Storage Media

Personal or sensitive data must not be stored on non-University removable media. Where strictly necessary, Childlight-approved encrypted USB drives may be issued by the Office Manager, provided that:

- The device is signed out and back in.
- It is wiped before return.
- It uses AES-256 encryption or equivalent.

Clean Device Services

Staff travelling to high-risk countries may request a university-provided "clean device" (temporary laptop/phone with no sensitive data). This should be flagged during travel risk assessment and arranged through the Office Manager.

7. Policy Review

The Childlight Data Management Policy is subject to regular review. Amendments are made to reflect changes in local practices, national and international policies, and professional best practice. This policy will also be reviewed and updated as necessary by Global Director of Data and/or the Quality and Compliance Manager, based on findings from internal audits and feedback from stakeholders. Any such amendments require the approval of the Childlight SLT.

This policy must be reviewed every two years. The review may result in one of three outcomes:

Approved	The policy has undergone changes which have been accepted by the Childlight SLT. Results in a change of version number.
Renewed	The policy was reviewed with no necessary changes identified. Does not result in a change of version number.
Discontinued	The policy was found to no longer hold relevance for the organisation, either as a result of content integration with other policy documents, or a change in operational need.

This policy was approved on 22nd September 2025
This policy is due for review on 21st September 2027

Appendix 1: Childlight Data Sharing Agreement Checklist

Sharing Data OUT of Childlight	Receiving Data INTO Childlight
Who is the data recipient?	Who is the data provider/partner?
Who is contact at the data recipient / other party	Contact at provider/partner
Do we have an existing partnership in place with the supplier/partner?	Do we have an existing partnership in place with the supplier/partner?
What type of data are being transferred?	What type of data are being transferred?
How was the data generated?	Who needs access within Childlight?
Who funded the generation/acquisition of the data?	What are the data being used for?
Are the data part of a larger data repository?	Are the data being used for a wider project?
What will the data recipient use the data for?	Are Personal Data being transferred?
Who at the data recipient requires access to the data?	Are pseudonymised / de-identified data relating to people being transferred / accessed?
Is the data recipient's project a standalone independent project or a collaborative project?	Do you have REC approval for the use of the data in the project?
Are identifiable personal data being transferred / accessed?	Have you engaged the Quality and Compliance Manager within Childlight about this transfer?
Are pseudonymised / de-identified data relating to people being transferred / accessed?	Where will the data be stored?
Do you have REC approval for sharing the data?	Have you received a separate DSA or DTA from the partner/data provider?
Does the data recipient / other party require REC approval for its use of the data?	
What security measures are you requiring the other party to put in place and do you have evidence of this?	

Are there other restrictions or limitations on the use of the data by the external party?	
Do you need to receive any derived or resultant data following transfer of the data to the party?	
Who owns the derived data or results of the research conducted on the shared data?	
Does Childlight has a license to use and re-share the derived data or results of the research?	
Does the recipient need to comply with a specific publications policy etc.?	
Is the data sharing agreement time limited or critical?	

Appendix 2: Data Breach Reporting Form

To be completed by the person area reporting the data protection breach.

Question	Response
REPORTING THE POTENTIAL BREACH	
Name and job title of the person reporting the incident, and of the person completing this form (if different)	
Organisational unit (e.g., school/service)	
DISCOVERY OF THE POTENTIAL BREACH	
When did the incident/problem become known?	(Time and date)
Who initially discovered the incident/problem?	(If the discovery was made by a member of staff, provide name, job title and unit. If someone else discovered the incident please describe, noting if the incident involves their personal data)
How was the incident/problem discovered?	(E.g., Was a complaint received or did a member of staff discover the incident)
Has a complaint been received from the data subject(s) (i.e., the individual(s) who the information relates to)?	
NATURE AND CIRCUMSTANCES OF THE POTENTIAL BREACH	
Describe in detail the nature of the incident and the circumstances	(When, what, who, summary of incident etc.)
When did the incident/problem occur?	(Date and time of the incident with as much accuracy as reasonably possible, or the period in which the incident is known to have occurred.)
Categorise the type of incident/problem	Select/highlight the option that fits most closely: • Misdirected communication (e.g. sending an email or letter to the wrong recipients) • Mislaid data (e.g. leaving a paper file or portable device in a public place) • Theft of device/hardware containing data

	• Premature destruction or deletion of golden copy data contrary to the retention schedule • Unauthorised access to data (e.g., through hacking, phishing etc) • Unauthorised editing/amendment of data (e.g., by a disgruntled employee) • Other: please specify
Who are the data subjects?	Select/highlight all categories that apply: • Students • Staff • Research volunteers • Applicants to study • Job applicants • Alumni • Other: please specify

What format is the data?	Select/highlight all categories that apply:
	• Paper
	• Email with or without an attachment
	• Digital data on a removable/portable device:
	  ○ UoE owned laptop
	  ○ Personally owned laptop
	  ○ UoE owned tablet
	  ○ Personally owned tablet
	  ○ UoE owned smart phone
	  ○ Personally owned smart phone
	  ○ USB drive
	  ○ UoE owned PC
	  ○ Personally owned PC
	• Digital data on UoE server / cloud
	• Digital data on third party server / cloud
	• Other: please specify

What are the categories of personal data (provide and any further details)	Select/highlight all categories that apply:
	• Personal identifiers
	  ○ Name
	  ○ Date of birth
	  ○ Matriculation number
	  ○ Examination number
	  ○ Staff number
	  ○ Other: please specify

	• Contact details
	  ○ Home address
	  ○ Home/personal telephone number
	  ○ Home/personal email address
	  ○ Work address
	  ○ Work telephone number
	  ○ Work email address
	  ○ Other: please specify
	• Financial information
	  ○ Bank details
	  ○ Salary information
	  ○ Other: please specify
	• Progression information
	  ○ Marks / grades
	  ○ Appraisal / annual review information
	  ○ Other: please specify
	• Criminal convictions or offences
	• Special Category personal data
	  ○ Health (e.g., sickness absence information, including medical certificates; Special circumstances information; Disability information; medical records; and PVG information)
	  ○ Ethnic origin (e.g., staff and student ethnicity information)
	  ○ Political opinions
	  ○ Religious or philosophical beliefs
	  ○ Trade Union membership
	  ○ Sex life or sexual orientation
	  ○ Genetic or biometric data
	• Other: please specify

How many individuals does the incident concern and how many personal data records?	
In addition to the personal data is any other information involved? E.g., confidential business information	

Has anything similar happened before?	(Give details)
ACTIONS TAKEN	
What actions have been taken so far in response to the incident? If relevant, what is being done to recover the information and/or prevent the further transmission of the information and/or delete the information mistakenly disclosed?	(E.g., If information was sent electronically to an incorrect recipient(s), have they been asked to delete the information? If a device was lost or stolen and remote wipe is possible, has this been done? If a password has been disclosed, has it been changed?)
If applicable: what action was taken by the recipient when they inadvertently received the information?	
Have you already notified the data subjects?	(If so, explain how and attach correspondence)
POLICIES, PROCEDURES AND TRAINING IN PLACE AT THE TIME OF THE INCIDENT	
Describe in as much detail as possible, the safeguards that were in place to protect the data. Please state if a Data Protection Impact Assessment (DPIA) has been undertaken.	(E.g., Include details of relevant administrative/procedural measures, e.g. policies, standard operating procedures and working practices, and IT security measures, e.g. encryption)
Have the relevant members of staff undertaken data protection training? (Provide details)	(E.g., Have they undertaken the mandatory online Data Protection and Information Security Essentials training courses?)