Byram House

ELECTRONIC RECORDS AND ACCESS POLICY

Date: May 2026

ELECTRONIC RECORDS AND ACCESS POLICY

Contents

1. Introduction to the Policy

This policy sets out the framework, principles, and procedures that **Byram House** follows for the creation, access, storage, and security of electronic records relating to children and young people in our care. The policy applies to all staff, agency workers, volunteers, contractors, and any external persons (e.g., Regulation 44 Visitors, Ofsted inspectors) who are granted access to the home's electronic recording system.

The Home is Byram House, which comprises the two residences at 62 Deighton Road and 66 Deighton Road. This policy applies equally across both residences.

The primary electronic recording system for children's records is **Clear Care**. This policy also applies to any other means of recording data electronically (e.g., email, shared drives, Bright HR for staff files – though staff files are covered separately). All electronic records must be managed in compliance with the **Data Protection Act 2018**, **UK GDPR**, and the **Children's Homes (England) Regulations 2015**.

The objectives of this policy are to:

- Ensure that electronic records are created, accessed, and stored securely.
- Define access levels based on legitimate need (role-based access control).
- Comply with Regulation 38 of the Children's Homes Regulations 2015 (records must be easily accessible to those with a legitimate need and reproducible in legible form).
- Protect the confidentiality, integrity, and availability of children's data.
- Prevent unauthorised access, loss, or damage to records.
- Provide a clear user agreement and disciplinary framework for breaches.

2. How this Policy Benefits the Home

This Electronic Records and Access Policy benefits Byram House in the following ways:

- **Legal Compliance** – It ensures compliance with the **Data Protection Act 2018**, **UK GDPR**, and **Regulation 38** of the Children's Homes Regulations 2015.
- **Data Security** – It defines clear security principles (confidentiality, integrity, availability) and mandates secure equipment, log-off procedures, and encrypted email.
- **Role-Based Access** – It prevents unauthorised access by restricting users to only the records they need for their role (e.g., Keyworkers only access children in their own home).
- **Audit Trail** – It requires regular scrutiny by Registered Managers and the Administration Support Team, creating an audit trail.
- **Business Continuity** – It requires backup and business continuity planning to prevent loss of records.
- **Inspection Readiness** – The **Social Care Common Inspection Framework (SCCIF) 2026** expects secure record keeping. This policy provides clear evidence.
- **Training Framework** – It sets out annual training for staff on data protection, access controls, and secure use of Clear Care.

3. Definitions & Legislation

3.1 Definitions

Term	Definition
Home	Byram House, the children's home registered with Ofsted, comprising two residences at 62 Deighton Road and 66 Deighton Road.
Company	IMS Care LTD, the registered provider and legal entity responsible for operating Byram House.
Byram House	The name used throughout this policy to refer to the home and its staff.
Clear Care	The home's primary electronic recording system for children's case records, daily logs, incident reports, and care planning documents.
Electronic Records	Any information relating to a child or young person that is created, stored, or transmitted electronically (including text, images, emails, and audio/video).
Legitimate Need	A lawful and justified reason for accessing a child's records, based on the individual's role and responsibilities.
Data Protection Act 2018	The UK's implementation of the GDPR, governing the processing of personal data.
UK GDPR	The retained EU law version of the General Data Protection Regulation, as amended by the Data Protection Act 2018.
Regulation 38	The provision in the Children's Homes (England) Regulations 2015 requiring that records be kept securely and be accessible to authorised persons.

Business Continuity Plan (BCP)	A plan to prevent loss or damage to records and to restore access in the event of a system failure.

3.2 Key Legislation and Statutory Guidance (presented in a table)

Legislation / Guidance	Key Provisions	Relevance to this Policy
Data Protection Act 2018	Sets out the legal framework for processing personal data, including data protection principles, individual rights, and the role of the Information Commissioner.	All electronic records must be processed lawfully, fairly, and transparently.
UK GDPR	Requires a lawful basis for processing, data minimisation, purpose limitation, storage limitation, integrity and confidentiality.	The home must have a lawful basis for processing children's data (e.g., legal obligation, legitimate interests).
Children's Homes (England) Regulations 2015 – Regulation 38	Records may be kept electronically provided they are easily accessible to those with a legitimate need, reproducible in legible form, and protected against loss or damage.	This policy operationalises Regulation 38.
Working Together to Safeguard Children 2026	Emphasises the importance of timely and secure information sharing for safeguarding.	Electronic records must be accessible to safeguarding partners when needed.

Social Care Common Inspection Framework (SCCIF) 2026	Inspects the home's record keeping and data security.	Inspectors will review electronic records and access controls.
Computer Misuse Act 1990	Makes it an offence to access computer material without authorisation.	Staff who access records without legitimate need may be committing an offence.
Freedom of Information Act 2000	Gives individuals the right to request information from public authorities (not directly applicable to children's homes but relevant for transparency).	The home should be prepared to respond to subject access requests (under UK GDPR).

4. The Policy

4.1 Policy Statement and Scope

Byram House will maintain electronic records for each child and young person in accordance with the **Data Protection Act 2018**, **UK GDPR**, and **Regulation 38** of the Children's Homes Regulations 2015.

All electronic records must be:

- **Accurate** and kept up-to-date.
- **Secure** from unauthorised access, loss, or damage.
- **Accessible** to those with a legitimate need (e.g., the child's Keyworker, Registered Manager, social worker, placing authority, Ofsted inspectors).
- **Reproducible** in legible form (e.g., printable) when required.

This policy applies to:

- All employees of Byram House (IMS Care LTD).
- Agency workers, volunteers, and contractors.
- External persons granted access (e.g., Regulation 44 Visitors, Ofsted inspectors, placing authority officers).

The primary system for children's electronic records is **Clear Care**. Any other electronic recording (emails, spreadsheets, documents) must also comply with this policy.

4.2 The Electronic Recording System (Clear Care)

Clear Care is the approved system for:

- Daily logs and summaries.
- Incident reports and physical intervention records.
- Care plans, risk assessments, and ISPs.
- Health records and appointment logs.
- Missing episode records.
- Complaints and compliments.

All staff must use Clear Care for these purposes. No children's records shall be stored on personal devices, unencrypted USB drives, or non-approved cloud services.

4.3 Authorised Equipment and Devices

- **Approved devices only:** Electronic records may only be accessed on devices approved and authorised by IMS Care LTD (e.g., home-owned desktop PCs, laptops issued by the company).
- **Personal devices (including mobile phones, tablets, personal laptops) are strictly prohibited** for accessing or completing children's records.
- **Remote access:** Staff with approved remote access must ensure their home device (if company-issued) is secure, password-protected, and used only by the authorised individual. The home reserves the right to request the IP address and security specification of any remote device.

4.4 Data Security Principles (Confidentiality, Integrity, Availability)

Staff must maintain the **CIA triad**:

Principle	Application
Confidentiality	Only people with a legitimate need can access data. Staff must log off from their PC when leaving it unattended. Monitors must not show confidential information to passers-by.
Integrity	Data must be accurate and suitable for its purpose. Records must not be altered without authorisation. Any corrections must be made as a new entry (audit trail).
Availability	Authorised users must be able to access data when needed. The home maintains a Business Continuity Plan (BCP) and regular backups to prevent loss.

4.5 Access Levels and User Roles

Access to Clear Care is role-based and restricted to **legitimate need**. The table below sets out standard access levels:

Role	Access Level	Notes
Residential Support Worker / Keyworker	Read and write for children in their assigned home (62 or 66 Deighton Road). Cannot access children in the other residence unless temporarily assigned.	Sessional / agency staff have access only for the days they are on shift.
Team Leader / Deputy Manager	Read and write for all children in the home (both 62 and 66 Deighton Road).	May also have access to management reports.

Registered Manager	Full read/write for all children in both residences.	Also access to system administration (user permissions, limited).
Registered Manager (other homes – if applicable)	Read only for children in this home (with legitimate need).	Must seek permission from the home's manager.
Education Staff (if employed by home)	Read only for education-relevant information (e.g., PEP, attendance) for children enrolled.	Cannot access unrelated health or safeguarding records.
Clinical / Therapy Staff	Read/write for children allocated to them for consultation.	Access limited to those children.
On Call Manager (regional)	Read only for children in the region (for emergency purposes).	May be granted write access in exceptional circumstances (recorded).
Placing Authority / Social Worker	Read only for children placed by that authority.	Access granted via secure portal or read-only account.
Ofsted Inspector	Read only (on request during inspection).	Access granted at the time of inspection.
Regulation 44 Independent Visitor	Read only (once approval is obtained from placing authorities, preferably at placement planning meeting).	Access must be logged.

Responsible Individual, Regional Manager, Quality & Compliance Manager, CEO	Full read access; limited write access (as needed).	
Administration Support Team (Clear Care)	Full system access for technical maintenance.	Strictly controlled; all actions logged.

Prior to sharing any child's information with another service (e.g., internal referral), the Registered Manager must obtain permission from the child's social worker as confirmation of legitimate need.

4.6 User Agreement and Passwords

Before being granted access to Clear Care, every user (including external persons) must **sign a User Agreement** (Appendix A, held electronically). The agreement confirms:

- Their role and permitted access level.
- That they will keep their password secure and not share it.
- That they will log off when leaving a device.
- That they understand the consequences of unauthorised access (disciplinary action, potential criminal offence under the Computer Misuse Act 1990).

Passwords must:

- Be strong (minimum 8 characters, with a mix of letters, numbers, and symbols).
- Not be written down or shared.
- Be changed periodically (as required by the system).
- Be for the named user only – sharing passwords is prohibited.

4.7 Remote Access and Home Working

Staff with approved remote access (e.g., managers, Quality & Compliance staff) must:

- Use only a **company-issued, encrypted device** (laptop) with up-to-date antivirus and firewall.
- Ensure their home internet connection is secure (password-protected Wi-Fi).
- Not work with confidential records in public places (e.g., cafés, libraries, public transport).
- Log off immediately after finishing work.
- Report any loss or theft of a device immediately to the Registered Manager and the IT Support team.

The Administration Support Team reserves the right to request the IP address and security specification of any remote device.

4.8 Sharing Information and Print Management

- **Email sharing:** When sending emails containing links to children's data or attachments with personal information, staff must use the **secure email facility** (encrypted) and only send to recipients with a legitimate need.
- **Printing:** Records must **not** be printed unless there is a legitimate reason (e.g., for a child-focused meeting where an electronic device is not available). Printed records must be:
    - Shredded immediately after the meeting.
    - Not left unattended.
- **External bodies (e.g., placing authority)** with agreed read-only access may view records online; physical copies should not be provided unless requested and approved by the Registered Manager.

4.9 Monitoring and Scrutiny

- **Registered Manager** – Must perform regular (no less than **monthly**) checks on Clear Care to ensure adherence to access controls and record-keeping standards. Any concerns must be raised with the Administration Support Team.
- **Responsible Individual** – Will review access logs as part of the governance framework.
- **Audit trails** – Clear Care maintains an audit trail of who accessed which record and when. The home will cooperate with any investigation into unauthorised access.

4.10 Business Continuity and Data Backup

- Clear Care data is backed up daily (by the system provider) and stored securely.
- The home has a **Business Continuity Plan (BCP)** to prevent loss or damage to records. In the event of a system failure, the home will follow the BCP to ensure continuity of care and record keeping.
- Printed emergency records (e.g., key contact numbers, medication lists) are kept in a locked cabinet for use only during system downtime.

4.11 Breaches and Disciplinary Action

Unauthorised access to electronic records is a serious matter and may constitute:

- A breach of this policy and the Data Protection Act 2018.
- A criminal offence under the Computer Misuse Act 1990.
- Gross misconduct under the Disciplinary Policy.

Actions for non-compliance:

Breach	Consequence

Sharing password with another person	Disciplinary action (written warning to dismissal, depending on severity)
Accessing records without legitimate need (e.g., curiosity)	Gross misconduct – immediate dismissal possible
Using a personal device to access records	Gross misconduct
Failure to log off, leaving records visible	Written warning (or final warning)
Unauthorised disclosure of child's data to a third party	Gross misconduct and potential ICO reporting

All breaches must be reported immediately to the Registered Manager. The home will notify the Information Commissioner's Office (ICO) within 72 hours where the breach is likely to result in a risk to individuals' rights and freedoms.

5. How the Home Trains its Staff About this Policy

Byram House provides structured training to ensure all staff understand and can implement this Electronic Records and Access Policy effectively.

Training Element	Frequency	Method / Content
Induction	Upon appointment	Face-to-face training covering: data protection principles (DPA 2018, UK GDPR), Regulation 38, use of Clear Care, role-based access controls,

		password security, secure email, printing rules, logging off, breach reporting, and the dual-site operation (62 & 66 Deighton Road).
Annual refresher	Every 12 months	Classroom or virtual session covering updates to legislation (ICO guidance, SCCIF 2026), case studies of data breaches, and refresher on access control.
Clear Care practical training	At induction and as needed	Hands-on training on using Clear Care, completing records, running reports, and understanding audit trails.
Data protection and SARs	At induction and biennially	Training on handling subject access requests, redaction, and ICO reporting obligations.

Staff are required to:

- Read and sign this policy annually.
- Complete all mandatory training.
- Sign the User Agreement before receiving a password.
- Immediately report any suspected unauthorised access.

6. Related Policies and Guidance

- Data Protection Policy
- Confidentiality Policy
- Whistleblowing Policy
- Disciplinary Policy
- Incident Reporting Policy
- Information Security Policy (if separate)
- Children’s Homes (England) Regulations 2015 (Regulation 38)
- Working Together to Safeguard Children 2026
- Social Care Common Inspection Framework (SCCIF) for Children’s Homes 2026
- ICO guidance on data protection

7. Policy Approval and Review Details

Byram House

Home	Byram House	
Reviewed by	Danyaal Iqbal / Mustafa Amin	Deputy Manager / Registered Manager
Approved by	Stacey Wagstaffe	Responsible Individual
Date	May 2026	