Byram House

CONFIDENTIALITY POLICY

Date: May 2026

CONFIDENTIALITY POLICY

Contents

1. Introduction to the Policy

This policy sets out the framework, principles, and procedures that **Byram House** follows to maintain the confidentiality of all information relating to children and young people in our care, employees, stakeholders, business partners, and any other information pertinent to the business. The policy applies to all employees, agency workers, volunteers, contractors, and anyone acting on behalf of Byram House, whether at 62 Deighton Road, 66 Deighton Road, or elsewhere.

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.

Justification for maintaining confidentiality is necessary for a condition of trust. Byram House is committed to maintaining the privacy of its employees and those it looks after. This policy must be observed by all associated with the home.

It is the responsibility of the management team to ensure that all staff members are aware of and understand this policy.

2. How this Policy Benefits the Home

This Confidentiality Policy benefits Byram House in the following ways:

- **Legal Compliance** – It ensures the home meets its obligations under the **Data Protection Act 2018**, the **UK GDPR**, the **Human Rights Act 1998**, the **Common Law Duty of Confidentiality**, the **Employment Rights Act 1996** (as amended), and the **Working Together to Safeguard Children 2026**. It also aligns with the **Social Care Common Inspection Framework (SCCIF) 2026** expectation that information is handled safely and transparently.
- **Child Protection** – It clarifies when information may be shared without consent (e.g., safeguarding concerns, prevention of serious crime, public interest), ensuring that data protection is not a barrier to protecting children.
- **Trust and Professionalism** – It builds trust with children, families, and placing authorities by demonstrating a commitment to handling personal information sensitively and securely.
- **Risk Reduction** – It sets clear rules for access on a 'need to know' basis, secure storage, remote working, and email communication, reducing the risk of accidental or intentional breaches.
- **Staff Accountability** – It makes clear that breaches of confidentiality may constitute gross misconduct, leading to dismissal or termination of contract, and that the home may seek civil damages.
- **Training Framework** – It sets out regular training for all staff on data protection, confidentiality, and information sharing.
- **Inspection Readiness** – The **SCCIF 2026** expects homes to have robust information governance. This policy provides clear evidence of compliance.

---

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.
Confidentiality	The duty to protect information received through formal channels, informally, or discovered by accident, and to not disclose it without proper authorisation unless required by law or justified in the public interest.
Information	All information relating to children, young people, employees, stakeholders, business partners, and the business of Byram House, held in any form (written, electronic, verbal, visual).
Personal Data	Any information relating to an identified or identifiable living individual (Data Protection Act 2018).
Special Category Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, or data concerning sex life or sexual orientation.
Informed Consent	Consent freely given, specific, informed, and unambiguous, with a clear affirmative action (UK GDPR).

Need to Know	The principle that access to sensitive information should be restricted only to those individuals who require it to perform their professional duties in the best interests of the child or the home.
Common Law Duty of Confidentiality	A legal obligation arising from case law that information obtained in confidence must not be used or disclosed without lawful authority or justification.
Public Interest Disclosure	A disclosure made for the purpose of preventing harm to the public (including children) that may override the duty of confidentiality.
Gross Misconduct	A breach of confidentiality so serious that it justifies summary dismissal without notice.

3.2 Key Legislation and Statutory Guidance

Legislation / Guidance	Key Provisions	Relevance to this Policy
Data Protection Act 2018 (DPA 2018)	The UK's implementation of the GDPR, supplementing it with domestic provisions. Sets out the legal framework for processing personal data, including special category data. Applies to controllers and processors.	Byram House is a data controller. The policy must comply with the DPA 2018 principles and lawful bases for processing.
UK General Data Protection Regulation (UK GDPR)	Retained EU law as amended by the DPA 2018. Governs the processing of personal data. Key principles: lawfulness, fairness, transparency; purpose limitation; data	All handling of personal data must follow these principles. Staff must understand their obligations.

	minimisation; accuracy; storage limitation; integrity and confidentiality (security).	
Human Rights Act 1998	Article 8 – right to respect for private and family life, home, and correspondence. Article 10 – freedom of expression (including right to receive and impart information, subject to restrictions).	Confidentiality is a fundamental aspect of the right to privacy. Any interference (e.g., sharing information) must be lawful, necessary, and proportionate.
Common Law Duty of Confidentiality	Developed through case law. A duty of confidence arises where information is given in circumstances where the recipient ought to know it is confidential. The duty can be overridden in the public interest (e.g., to prevent serious crime or harm to children).	This policy explicitly recognises that safeguarding concerns override confidentiality. Staff must not use confidentiality as a barrier to sharing information to protect a child.
Children Act 1989	Section 47 – duty to investigate where a child is suffering or likely to suffer significant harm. Section 22 – duty to safeguard and promote the child's welfare.	Information sharing for child protection purposes is not only permitted but required under these statutory duties.
Working Together to Safeguard Children 2026	Published March 2026. Reinforces that data protection is not a barrier to sharing safeguarding information. Stresses the need for timely sharing with relevant professionals.	Staff must understand that safeguarding concerns must always be passed on, and consent is not required where there is a lawful basis.

Social Care Common Inspection Framework (SCCIF) for Children's Homes 2026	Effective 1 April 2026. Expects homes to have effective systems for information governance, including secure storage and appropriate sharing.	Inspectors will review how the home handles confidential information, including records management and data sharing.
Employment Rights Act 1996 (as amended by Public Interest Disclosure Act 1998 and Employment Rights Act 2025)	Protects employees who make qualifying disclosures (whistleblowing) from detriment or dismissal. From 6 April 2026, includes sexual harassment as a protected category.	Staff who raise concerns about breaches of confidentiality or other wrongdoing are protected.
Caldicott Principles (applied in health and social care)	Seven principles: justify purpose; don't use unless necessary; use minimum necessary; need to know access; everyone understands their duty; comply with law; duty to share for individual and public interest.	These principles underpin the 'need to know' and 'minimum necessary' approach in this policy.

4. The Policy

4.1 Purpose and Scope

The purpose of this policy is to assist all staff and those working on behalf of Byram House to understand their duties of confidentiality towards the organisation and the children and families we serve.

This policy applies to all employees, agency workers, volunteers, contractors, and any person authorised by the home to have access to information. It applies to information received through formal channels, informally, or discovered by accident, held in any form (written, electronic, verbal, visual).

The policy is applied without discrimination, irrespective of age, ethnicity, gender, marital or civil partnership status, nationality, offending history, race, disability, religion or belief, sexual orientation, social status, trade union membership, or working patterns.

Any breach of confidentiality will be treated as gross misconduct potentially justifying summary dismissal (for employees) or immediate termination of contract (for contractors). The commitment to confidentiality **continues even after employment or contract ends**. The home reserves the right to seek civil damages for any loss or expense resulting from a breach.

If at any point a staff member is unsure about any aspect of this policy, they must discuss the matter with the management team or Human Resources.

4.2 Responsibilities

Role	Responsibilities
All Staff and Contractors	– Treat all information relating to children, families, employees, and the business as strictly confidential. – Not access information for which they do not have a legitimate reason in the course of their duties. – Not share confidential information with third parties without prior managerial agreement, unless required by law or for safeguarding. – Abide by the terms of this policy and any contract of employment or service. – Report any breach or suspected breach immediately to their line manager.
Line Managers	– Ensure their team members are aware of and understand this policy. – Authorise appropriate sharing of information where necessary and lawful. – Investigate any alleged breaches and escalate to HR/management.
Registered Manager	– Overall responsibility for implementing this policy within the home. – Ensure secure storage systems are maintained. – Act as the first point of contact for complex confidentiality decisions.
Directors and Responsible Individual	– Ensure the home has adequate training and resources to comply with data protection law. – Make decisions on disciplinary action following serious breaches.

4.3 Data Protection Principles (DPA 2018 & UK GDPR)

All processing of personal data must comply with the following principles:

Principle	Application
Lawfulness, fairness, transparency	Process personal data lawfully (using a lawful basis, e.g., consent, legal obligation, public task, legitimate interests). Be transparent with children and families about how their data is used (privacy notice).
Purpose limitation	Collect data for specified, explicit, and legitimate purposes only. Do not use for incompatible purposes.
Data minimisation	Ensure data is adequate, relevant, and limited to what is necessary for the purpose.
Accuracy	Take reasonable steps to ensure personal data is accurate and, where necessary, kept up to date. Correct or erase inaccurate data without delay.
Storage limitation	Keep data only for as long as necessary for the purpose. Set and follow retention schedules.
Integrity and confidentiality (security)	Process data in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage.
Accountability	Be able to demonstrate compliance with all the above principles. Maintain records of processing activities.

4.4 Maintaining Confidentiality – Key Obligations

4.4.1 Duty of Care

All staff must show respect for their colleagues and the work they undertake, and understand the need for privacy and confidentiality.

- **Email communication:** Particular care should be taken when drafting emails. Do not forward or copy messages or attachments containing personal/sensitive information without the originator's permission. Blind copying (Bcc) should be used judiciously; misuse may risk defamation or breach of confidence.
- **Approaches about employment:** If a staff member is approached by someone they know (or are linked to) about employment with the home, they should not disclose any internal information. Instead, advise the person to apply through official channels. Consult the line manager for guidance.
- **Unsolicited requests for information:** If a staff member is asked for confidential information by someone they know, they must **not** provide any information without authorisation. Refer the request to the line manager and follow the guidance in this policy.

4.4.2 Need to Know

Sensitive information must only be requested and accessed on a **'need to know'** basis. This means:

- The information is necessary to provide a service to the child or to perform the staff member's professional duties.
- Access is in the best interests of the child or the legitimate purposes of the home.
- Only the minimum amount of information necessary should be shared.

4.4.3 Informed and Explicit Consent

- Where information is confidential and restricted, it should only be passed on to unauthorised persons where the **informed and explicit consent** of the individual concerned has been obtained.

- **Informed consent** means the individual understands what information will be shared, with whom, for what purpose, and the potential consequences. Consent must be freely given and recorded.
- Whenever possible, consent should be **in writing** (including signed forms or recorded verbal agreement with a witness).
- **Telephone disclosures:** Confidential information should not be discussed on the telephone unless the identity of the caller is reliably established. If necessary, call back using a verified number.

4.4.4 Circumstances Where Information May Be Disclosed Without Consent

The duty of confidentiality can be overridden in certain circumstances. **Data protection is not a barrier to sharing safeguarding information.** Information may be shared without consent where:

- **There is a legal duty or statutory power** to share (e.g., Children Act 1989, Section 47; child protection referrals).
- **It is in the public interest** to prevent serious harm to a child or vulnerable adult, or to prevent or detect serious crime. This includes safeguarding concerns, exploitation, radicalisation, FGM, and forced marriage.
- **The disclosure is required by a court order** or other legal process.
- **The information is needed for the 'team around the child'** to provide effective care (provided the sharing is proportionate and necessary).
- **The child lacks capacity** to consent and sharing is in their best interests (following the Mental Capacity Act 2005 principles, though most children in care are over 16 or have Gillick competence considerations – always consult the DSL or manager).

Difficult decisions should be discussed with a Line Manager, the Designated Safeguarding Lead, or the Responsible Individual. They may need to seek legal advice.

Important: The **Common Law Duty of Confidentiality** is not absolute. The overriding duty to safeguard children always takes precedence. Staff should never withhold information about a safeguarding concern because they do not have consent.

4.5 Secure Storage and Handling of Information

- **Physical records:** All paper files containing personal or confidential information must be kept in lockable filing cabinets or secure rooms. Access should be restricted to authorised personnel.
- **Electronic records:** The home's electronic recording system (Clear Care) is password-protected. Staff must log off when away from their workstation. No passwords should be shared.
- **Remote working / working from home:** Extra care must be taken. Staff should:
    - Use only encrypted devices approved by the home.
    - Not leave confidential documents visible or unsecured.
    - Use secure VPN connections when accessing home systems.
    - Not use personal email or cloud storage for work-related confidential information.
- **Retention:** Personal data must only be kept for as long as necessary, in accordance with the home's Data Protection Policy and retention schedule.
- **Disposal:** Paper records must be shredded (cross-cut) before disposal. Electronic records must be permanently deleted using secure deletion methods.

4.6 Breaches of Confidentiality

A breach of confidentiality occurs when sensitive information is given to people who are not authorised to access it, or when procedures are not followed, whether intentionally or accidentally.

Examples of breaches include:

- Discussing a child's personal information in a public place where it can be overheard (e.g., lift, café, public transport).
- Leaving confidential documents on a desk, in a car, or in a home office where unauthorised persons can see them.
- Losing an unencrypted laptop or USB stick containing personal data.
- Sending confidential information to the wrong recipient by email or post.

- Accessing records for reasons unrelated to work (e.g., curiosity about a colleague or child you do not support).
- Sharing login credentials or leaving a terminal logged in.
- Disclosing information to a family member or friend without proper authorisation.

Consequences of a breach:

- Breaches can cause serious harm: discrimination, harassment, inappropriate decisions, reputational damage to the home, and safeguarding risks.
- Any breach of confidentiality by an employee will be treated as **gross misconduct** and may justify summary dismissal.
- For contractors, breach will lead to immediate termination of the contract.
- The home may bring civil proceedings to restrain further disclosure and claim damages for any loss or expense incurred.
- Serious breaches involving criminal behaviour (e.g., selling data) may be reported to the police and the Information Commissioner's Office (ICO).

If a breach occurs or is suspected:

1. **Report immediately** to the Line Manager or Registered Manager.
2. **Contain the breach** – attempt to recover any lost information, recall misdirected emails, or disable access.
3. **Assess the risk** – what information was involved, who has accessed it, what harm could arise.
4. **Notify affected individuals** if appropriate (e.g., the child or family).
5. **Report to the ICO** within 72 hours if the breach is likely to result in a risk to the rights and freedoms of individuals (e.g., sensitive data loss).
6. The home will investigate and take appropriate disciplinary or legal action.

All breaches, including near misses, must be recorded on the home's incident reporting system.

5. How the Home Trains its Staff About this Policy

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

Training Element	Frequency	Method / Content
Induction	Upon appointment	Face-to-face training covering: definitions of confidentiality, legal framework (DPA 2018, UK GDPR, Human Rights Act, common law duty), data protection principles, need to know, consent, circumstances for sharing without consent (safeguarding), secure storage, breach procedures, and the dual-site operation (62 & 66 Deighton Road).
Annual refresher	Every 12 months	Classroom or virtual session covering updates to legislation (Working Together 2026, SCCIF 2026, ICO guidance), case studies of real breaches, and reminders on email security and remote working.
Safeguarding information sharing	Annually	Specific training on when confidentiality can be overridden in the public interest, how to share information for child protection without consent, and the Caldicott principles.
Data protection and GDPR	Annually	Training on the UK GDPR principles, individual rights (access, rectification, erasure), lawful bases, and how to handle subject access requests (SARs).
Secure handling and remote working	At induction and as needed	Training on encryption, password security, secure disposal, and the risks of home/remote working.

Breach reporting	At induction and refresh	Training on recognising a breach, containing it, reporting internally, and ICO notification duties.
Record keeping	Ongoing	All training recorded on staff personnel files; managers monitor compliance.

Staff are required to:

- Read and sign this policy annually.
- Complete all mandatory training sessions.
- Immediately report any breach or suspected breach.
- Never use confidentiality as a reason to withhold safeguarding information.

6. Related Policies and Guidance

This policy must be read in conjunction with:

- Safeguarding Policy
- Data Protection Policy (including privacy notices and retention schedule)
- Whistleblowing Policy
- Code of Conduct and Ethics Policy
- Disciplinary Policy and Procedure
- IT and Internet Safety Policy
- Record Keeping Policy
- Children's Homes (England) Regulations 2015
- Working Together to Safeguard Children 2026
- Social Care Common Inspection Framework (SCCIF) for Children's Homes 2026
- ICO guidance on data sharing and breach reporting

7. Policy Approval and Review Details

Byram House

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