



SEXTORTION POLICY

Date: May 2026

SEXTORTION POLICY

Contents

1. Introduction to the Policy
2. How this Policy Benefits the Home
3. Definitions & Legislation
 - 3.1 Definitions
 - 3.2 Key Legislation and Statutory Guidance (table)
4. The Policy
 - 4.1 Policy Statement
 - 4.2 Prevention Measures (Education, Training, Boundaries, Monitoring)
 - 4.3 Reporting Procedures
 - 4.4 Response Protocol (Risk Assessment, Investigation, Follow-Up)
 - 4.5 Support for Victims
 - 4.6 Responsibilities of Children, Staff and DSL
5. How the Home Trains its Staff About this Policy
6. Related Policies and Guidance
7. Policy Approval and Review Details

1. Introduction to the Policy

This policy sets out the framework, principles, and procedures that **Byram House** follows to protect children and young people from the risks and harms associated with **sextortion**. The policy applies to all staff, agency workers, volunteers, and contractors working at 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.

Sextortion is a form of online sexual exploitation and blackmail. It involves coercing a person into sharing explicit images, videos, or engaging in sexual acts under threat of exposing the material to others. Children in residential care may be particularly vulnerable due to their histories of trauma, instability, and online exposure.

This policy is to be read in conjunction with the **Child/Young Person Sexual Abuse and Exploitation Policy** (CSE) and the **Internet Policy for Adults, Children and Young People**.

The objectives of this policy are to:

- Raise awareness among children and staff about the risks of sextortion.
- Establish clear protocols for reporting, responding to, and managing cases of sextortion.
- Ensure that children feel supported and empowered to report incidents without fear of blame.
- Provide appropriate interventions to mitigate harm and prevent further incidents.
- Comply with all relevant legislation, including the **Online Safety Act 2023**, the **Serious Crime Act 2015**, and **Working Together to Safeguard Children 2026**.

2. How this Policy Benefits the Home

This Sextortion Policy benefits Byram House in the following ways:

- **Legal Compliance** – It meets duties under the **Online Safety Act 2023** (protecting children from illegal and harmful content), the **Serious Crime Act 2015** (criminalisation of revenge porn and coercive behaviour), and the **Children's Homes Regulations 2015**.
- **Child Protection** – It provides a clear pathway for identifying, reporting, and responding to sextortion, ensuring that children are not blamed for their victimisation.
- **Prevention** – It includes education for children (safe online practices, boundaries) and training for staff (recognising signs, handling disclosures).
- **Multi-Agency Working** – It aligns with local safeguarding partnerships (MASH) and law enforcement procedures.
- **Victim Support** – It commits to providing emotional, psychological, and (where necessary) legal support to victims.
- **Inspection Readiness** – The **SCCIF 2026** expects the home to manage online risks effectively. This policy provides clear evidence.
- **Training Framework** – It sets out annual training for staff on sextortion, disclosure handling, and referral pathways.

3. Definitions & Legislation

3.1 Definitions

Term	Definition
Home	Byram House, comprising 62 Deighton Road and 66 Deighton Road.
Company	IMS Care LTD.
Byram House	The name used throughout this policy to refer to the home and its staff.
Sextortion	A type of sexual exploitation where a person is coerced into sharing explicit images, videos, or engaging in sexual acts under threat of harm, exposure, or manipulation. It is a form of blackmail.
Coercion	The act of using pressure, threats, or manipulation to force someone into a particular behaviour.
Sexual Exploitation	The abuse of power to manipulate someone into engaging in sexual activities for personal gain (including financial gain or sexual gratification).
Child Sexual Exploitation (CSE)	A form of sexual abuse in which a person takes advantage of a power imbalance to force or entice a child into sexual activity in return for something (gifts, money, affection, etc.).
Revenge Porn	The disclosure of private sexual photographs or films with intent to cause distress (criminal offence under section 33 of the Criminal Justice and Courts Act 2015, now consolidated into the Serious Crime Act 2015).

Youth Produced Sexual Imagery (Sexting)	The creation and sharing of sexual images or videos by young people under 18. This can be a pathway to sextortion if the images are used as leverage.
DSL	Designated Safeguarding Lead (the person responsible for managing safeguarding concerns, including sextortion).

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

Legislation / Guidance	Key Provisions	Relevance to this Policy
Online Safety Act 2023	Fully implemented 25 July 2025. Requires regulated online services to protect children from illegal and harmful content, including grooming, image-based abuse, and sextortion.	The home must educate children about reporting mechanisms and support them in using online reporting tools.
Serious Crime Act 2015 – Section 33	Criminalises the disclosure of private sexual photographs or films with intent to cause distress ("revenge porn").	Sextortion often involves threats to disclose such images. This is a criminal offence.
Serious Crime Act 2015 – Section 68	Creates an offence of possession of "paedophile manuals" (guides to grooming).	Not directly relevant but demonstrates the legal framework around online exploitation.

Malicious Communications Act 1988 / Communications Act 2003	Make it an offence to send threatening or offensive messages online.	Threats made during sextortion are criminal.
Protection from Harassment Act 1997	Harassment (including cyber-harassment) is a criminal offence.	Sextortion typically involves a course of conduct causing distress.
Children's Homes (England) Regulations 2015 – Regulation 34	Requires the home to have policies for the protection of children, including online safety.	This policy supports that requirement.
Working Together to Safeguard Children 2026	Emphasises multi-agency response to extra-familial harms, including online exploitation.	The home must work with MASH, police, and specialist services.
Social Care Common Inspection Framework (SCCIF) 2026	Inspects the home's management of online risks and exploitation.	Inspectors will review this policy and staff awareness.
UK Council for Internet Safety (UKCIS) – Sharing Nudes and Semi-Nudes Advice (2024)	Guidance for professionals on responding to sexting incidents.	Sextortion often arises from sexting. This advice must be followed.

4. The Policy

4.1 Policy Statement

Byram House takes a zero-tolerance approach to sextortion. We will:

- **Educate** children and staff about the risks of sextortion and how to stay safe online.
- **Prevent** through clear rules on device use, monitoring (in line with the Internet Policy), and promoting healthy relationships.
- **Identify** signs of sextortion through staff vigilance and children's disclosures.
- **Respond** swiftly and sensitively, ensuring that the child is not blamed, and that law enforcement and safeguarding partners are involved where necessary.
- **Support** victims with counselling, advocacy, and legal advice.

4.2 Prevention Measures

4.2.1 Education and Awareness

- Children will receive age-appropriate education on:
 - The risks of sharing explicit images or personal information online.
 - How to recognise coercion, threats, and manipulation.
 - The importance of not engaging with strangers who request sexual content.
 - How to report concerns (to staff, Childline, CEOP, Report Harmful Content).
- Keyworking sessions will include discussions on online safety, healthy relationships, and consent.

4.2.2 Staff Training

- All staff will receive annual training on:

- Recognising signs of sextortion (e.g., child becoming withdrawn, secretive about phone, receiving money or gifts).
 - Handling disclosures (do not promise confidentiality; do not view or share images).
 - Reporting procedures and the role of the DSL.
- The DSL will receive additional training on online exploitation and referral pathways.

4.2.3 Clear Boundaries (Device and Internet Use)

- The home's **Internet Policy** sets out rules for children's use of devices, including:
 - No sharing of personal information (address, school, phone number) with online contacts.
 - No sending of explicit images or videos.
 - Devices to be handed in at night (unless risk assessed otherwise).
 - Staff may check devices (browsing history, messages) as set out in the ISP.
- Children are made aware that monitoring is for their safety.

4.2.4 Monitoring and Auditing

- The home will regularly audit its internet filtering and monitoring systems to block access to known sextortion-related content.
- Staff will be alert to changes in a child's online behaviour (e.g., deleting messages, using secret apps, receiving unexplained gifts).

4.3 Reporting Procedures

Immediate Reporting

- If a child believes they are being targeted or coerced into sextortion, they should report it to a trusted staff member immediately.
- Staff must **take all disclosures seriously**. They must:

- Listen without judgement.
- **Do not promise confidentiality** – explain that they need to share the information to keep the child safe.
- **Do not view or share** any explicit images (if shown, look away and secure the device).
- Report to the **Designated Safeguarding Lead (DSL)** immediately (verbally, followed by written record on the same day).

Confidentiality

- Information will be shared only with those who need to know (e.g., DSL, child's social worker, police, MASH). The child will be informed of who will be told and why.

Support During Reporting

- The child will be offered a private space to talk, and an **advocate** may be requested.
- The home will not blame the child for having shared images initially.

4.4 Response Protocol

4.4.1 Risk Assessment

- The DSL will conduct an immediate risk assessment, considering:
 - What information has been shared and with whom.
 - Whether the perpetrator has made specific threats (e.g., to share images publicly).
 - Whether the child is at risk of immediate harm (suicidal ideation, self-harm).
 - Whether other children in the home may be at risk.
- A **safeguarding plan** will be implemented (e.g., temporarily restricting device use, increasing supervision, arranging a safety plan with police).

4.4.2 Investigation and Referral

- The DSL will make a referral to the **Kirklees MASH** (Front Door Safeguarding Hub) within **one working day** (or immediately if there is a risk of significant harm).
- The police will be notified (101 or 999) if a criminal offence has been committed (e.g., blackmail, harassment, distribution of indecent images).
- The child's social worker will be informed.
- The home will preserve evidence (e.g., screenshots of messages, but **without viewing** explicit images – the device will be secured and handed to police if required).
- **Ofsted** will be notified under Regulation 40 if the incident is serious (e.g., significant harm, police involvement, hospitalisation).

4.4.3 Follow-Up

- The DSL will maintain contact with the child, the social worker, and the police (if involved) to monitor the child's wellbeing.
- The child's ISP will be reviewed and updated to reflect any ongoing risks (e.g., restricted online access, additional support).

4.5 Support for Victims

Emotional and Psychological Support

- The home will offer immediate emotional support and arrange access to **counselling** (e.g., CAMHS, school counselling, or a specialist service for online exploitation).
- The child's Keyworker will provide regular one-to-one support.
- The home will signpost to external organisations:
 - **Childline** (0800 1111)
 - **CEOP** (www.ceop.police.uk) – report online grooming or exploitation.

- **Report Harmful Content** (<https://reportharmfulcontent.com>)
- **Revenge Porn Helpline** (www.revengepornhelpline.org.uk)

Legal Support

- If the child is involved in legal proceedings (as a victim), the home will work with the social worker and police to ensure the child has access to a **young person's legal advocate** or **witness support**.

Non-Judgmental Approach

- Staff will never blame the child for having taken or shared images. The focus is on the perpetrator's criminal behaviour.

4.6 Responsibilities of Children, Staff and DSL

Role	Responsibility
Children and Young People	– Follow the home's internet and device rules. – Report any suspicious contact or threats to staff immediately. – Do not share explicit images or personal information online.
All Staff	– Recognise signs of sextortion. – Take all disclosures seriously. – Report to DSL immediately. – Never promise confidentiality. – Do not view or share any explicit images shown by a child.
Designated Safeguarding Lead (DSL)	– Oversee implementation of this policy. – Conduct risk assessments.

	– Make referrals to MASH, police, and Ofsted. – Coordinate support for the victim. – Ensure the ISP is updated.
--	---

5. How the Home Trains its Staff About this Policy

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

Training Element	Frequency	Method / Content
Induction	Upon appointment	Face-to-face training covering: definition of sextortion, legal framework (Online Safety Act, Serious Crime Act), signs and indicators, reporting procedures (do not view images, preserve evidence, refer to DSL), risk assessment, support for victims, and the dual-site operation (62 & 66 Deighton Road).
Annual refresher	Every 12 months	Classroom or virtual session covering updates to legislation, case studies, and refresher on the response protocol.
DSL advanced training	As needed (at least every 2 years)	Training on online exploitation, digital evidence preservation, and working with police and MASH.

Online safety education	Annually	Training for staff on delivering age-appropriate education to children about sextortion, consent, and reporting.
--------------------------------	----------	--

Staff are required to:

- Read and sign this policy annually.
- Complete all mandatory training.
- Immediately report any suspicion of sextortion to the DSL.
- Never view or share explicit images shown by a child.

6. Related Policies and Guidance

- Child/Young Person Sexual Abuse and Exploitation Policy (CSE)
- Internet Policy for Adults, Children and Young People
- Safeguarding Policy
- Harmful Sexual Behaviours (HSB) Policy
- Bullying and Cyber Bullying Policy
- Incident Reporting Policy
- Notifications Policy (Regulation 40)
- Police Involvement Policy
- Children's Homes (England) Regulations 2015
- Working Together to Safeguard Children 2026
- Social Care Common Inspection Framework (SCCIF) for Children's Homes 2026
- UK Council for Internet Safety (UKCIS) – Sharing Nudes and Semi-Nudes Advice (2024)

7. Policy Approval and Review Details



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