Byram House

INTERNET POLICY

Date: May 2026

INTERNET POLICY

Contents

1. Introduction to the Policy

This policy sets out the framework, principles, and procedures that **Byram House** follows to ensure the safe use of the internet by children, young people, and adults (staff, volunteers, and visitors). The policy applies to all staff, agency workers, volunteers, contractors, and anyone acting on behalf of Byram House, whether at 62 Deighton Road, 66 Deighton Road, or elsewhere, including when using personal devices on the premises.

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 internet is an integral part of our lives. Children and young people must be kept safe from possible dangers and risks associated with the internet, while also needing to learn how to use it safely and effectively. The overarching emphasis of this policy is to provide guidance on how adults can help children and young people to achieve this, and to set clear expectations for adults' own online conduct.

This policy is based on the principle that we cannot make the internet completely safe (Byron Review, 2008), but we can educate children to make safe choices, understand risks, and know how to raise concerns and report inappropriate contact. It also recognises the legal duties under the **Online Safety Act 2023** (fully implemented from 25 July 2025), the **Data Protection Act 2018 & UK GDPR**, and the safeguarding framework of **Working Together to Safeguard Children 2026**.

Any breach of this policy by a staff member may result in disciplinary action, including gross misconduct.

2. How this Policy Benefits the Home

This Internet Policy benefits Byram House in the following ways:

- **Legal Compliance** – It ensures the home meets its duties under the **Online Safety Act 2023** (protecting children from illegal and harmful content online), the **Data Protection Act 2018 & UK GDPR** (processing of personal data), the **Children's Homes (England) Regulations 2015**, and **Working Together to Safeguard Children 2026**.
- **Child Protection** – It requires individual risk assessments, 1:1 supervision (unless risk-assessed otherwise), daily checks of browsing history and messages, and clear boundaries for internet use. It also provides a pathway for reporting online grooming, exploitation, or extremist content (CEOP, Report Harmful Content).
- **Staff Accountability** – It prohibits staff from sharing personal contact details or social media with children, requires personal devices to be stored securely during working hours, and forbids accepting friend requests from children. Breaches are gross misconduct.
- **Empowerment and Education** – It encourages staff to teach children how to keep themselves safe online (e.g., through online safety courses, key working conversations). It also provides a list of resources (CEOP, Thinkuknow, Net Aware, Report Harmful Content, etc.).
- **Risk-Based Approach** – It requires the Registered Manager to ensure that children's ISPs and risk assessments include internet-specific risks (e.g., access to inappropriate content, grooming, radicalisation, sexting). For children under 13, social networking is prohibited unless specifically risk-assessed and agreed.
- **Monitoring and Supervision** – It mandates daily checks of devices (history, texts, WhatsApp groups) recorded on daily summaries, and allows temporary suspension of internet use as a proportionate consequence (with review within 72 hours).
- **Inspection Readiness** – The **Social Care Common Inspection Framework (SCCIF) 2026** expects homes to demonstrate effective online safety management. This policy provides clear evidence.
- **Training Framework** – It requires induction training on internet safety, annual refreshers, and bite-size team workshops.

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.
Internet	Global system of interconnected computer networks, accessed via devices such as smartphones, tablets, laptops, gaming consoles, and smart TVs.
Personal Device	Any electronic device capable of connecting to the internet that is owned by a staff member (e.g., personal mobile phone, tablet, smartwatch).
Social Networking Site	An online platform for creating and sharing content and connecting with others (e.g., Facebook, Instagram, TikTok, Snapchat, WhatsApp, Discord).
Online Safety Act 2023	UK legislation that imposes duties on online service providers to protect children from illegal and harmful content, fully implemented from 25 July 2025.
CEOP	Child Exploitation and Online Protection Command (part of the National Crime Agency).
Thinkuknow	An online safety education programme developed by CEOP.

Harmful Content	Content that is illegal (e.g., child sexual abuse material) or potentially harmful to children (e.g., self-harm, suicide, eating disorder promotion, hate speech).
Sexting (Youth Produced Sexual Imagery)	The creation and sharing of sexual images or videos by young people under 18.
Netiquette	The code of acceptable behaviour on the internet.
Safeguarding Concern (Online)	Any incident where a child may be at risk of grooming, exposure to pornography, radicalisation, cyber-bullying, or contact by a perpetrator online.

3.2 Key Legislation and Statutory Guidance

Legislation / Guidance	Key Provisions	Relevance to this Policy
Online Safety Act 2023	Fully implemented from 25 July 2025. Imposes duties on regulated services (social media, search engines, messaging apps) to protect children from illegal and harmful content. Ofcom has issued Children's Safety Codes of Practice.	The home must educate children about online risks and support them in using reporting mechanisms. Staff should be aware that platforms have legal duties to act on reports.
Data Protection Act 2018 & UK GDPR	Governs processing of personal data. Children's online activity may generate personal data.	The home must ensure that monitoring of internet use (e.g., checking history) is lawful and transparent. Children's devices may contain personal data – staff access must be justified.

Children's Homes (England) Regulations 2015	Regulation 23 – Health and Wellbeing. Quality Standards – safe environment, positive relationships.	The home must have policies to protect children from online harm as part of the safe environment.
Working Together to Safeguard Children 2026	Published March 2026. Emphasises multi-agency response to extra-familial harms, including online abuse, exploitation, and radicalisation.	Online safety concerns must be treated as safeguarding concerns and reported to the local authority and, where appropriate, CEOP.
Keeping Children Safe in Education (KCSIE) 2026 (proposed)	Expected September 2026. Strengthens guidance on peer-on-peer abuse, online safety, and sexting.	The home will adopt KCSIE principles, including not dismissing harmful online behaviour as "banter".
Social Care Common Inspection Framework (SCCIF) for Children's Homes 2026	Effective 1 April 2026. Focuses on children's lived experience and whether the home effectively manages online risks.	Inspectors will evaluate the home's internet safety policy, staff training, and monitoring practices.
Digital Economy Act 2017 (Part 3 on age verification for pornographic content)	Previously required age verification for online pornography; superseded by Online Safety Act but similar principles apply.	The home should ensure that children are not able to access adult content via home Wi-Fi (by using content filtering).
Serious Crime Act 2015	Section 67 – criminal offence of disclosing private sexual photographs or films with intent to cause distress ("revenge porn").	If a child becomes a victim of image-based abuse, staff must report to police.

Malicious Communications Act 1988 / Communications Act 2003	Criminal offences for sending threatening or offensive messages online.	Cyber-bullying may be a criminal offence. Staff should support victims and report to police.
Byron Review (2008) – "Safer Children in a Digital World"	Foundational report emphasising that the internet cannot be completely safe; children need education and empowerment.	This policy is built on the principle of empowering children to manage their own safety with adult support.

4. The Policy

4.1 General Principles – Empowering Safe Internet Use

- Children and young people need to be empowered to keep themselves safe. We cannot make the internet completely safe, but we can educate them to make safe choices and to ensure they know how to raise concerns and report inappropriate contact.
- Adults have a duty to model safe and responsible online behaviour at all times.
- All internet use by children must be guided by individual risk assessments, ISPs, and a negotiated **Home Internet Guidance** agreed with the child and their social worker.
- The home will use appropriate technical measures (e.g., content filtering, parental controls on Wi-Fi) to block access to illegal and harmful content, but these are not a substitute for supervision and education.

4.2 Personal Devices – Adults (Staff Responsibilities)

Storage of personal devices:

- Adults are permitted to have their own personal devices (mobile phones, tablets, smartwatches) on the premises, but **from the moment they start work, these devices must be stored safely in the designated locked cupboard or personal belongings area**.
- Personal devices must not be used during working hours except:
    - In a genuine emergency (with permission of the senior person on duty).
    - For a pre-arranged personal call (arranged with the senior person before the shift).
- Using a personal device while supervising children is a distraction and could lead to a safeguarding incident.

Prohibited actions:

- Staff must **never** share personal telephone/mobile numbers, social media addresses, email addresses, or passwords with children or young people.
- Staff must **never** accept a 'friend request' or follow a child on any social media platform (including TikTok, Instagram, Snapchat, Facebook, WhatsApp groups, Discord).
- Staff must **never** communicate with a child via personal messaging apps (except in an emergency using a work-issued phone, with manager's knowledge).
- Staff must **never** take or share photographs of children on personal devices (use home-owned devices only, with consent).

Consequences: Any breach of these rules will be treated as **gross misconduct** and may lead to summary dismissal.

4.3 Risk Assessment for Children and Young People

- When a child moves into the home, the Registered Manager and Keyworker must ensure that **internet-specific risks** are included in the child's **Individual Safety Plan (ISP)** and risk assessment.
- The risk assessment must consider:
    - Whether the child has a history of online grooming, sexting, cyber-bullying, or accessing harmful content.
    - Whether the child is at risk of radicalisation (Prevent duty) or exploitation (CSE, county lines) via online platforms.
    - The child's age, maturity, and understanding of online risks.
    - Whether the child has their own mobile device with a SIM card (mobile data can bypass home Wi-Fi filtering).
- **Default supervision level:** All children will be supervised on a **1:1 basis** by an adult when using internet-enabled equipment, **unless** the risk assessment states otherwise and has been agreed with the placing authority (social worker). If the risk assessment permits independent internet use, it must specify the circumstances, time limits, and any monitoring required.

Checking devices:

- All equipment used by children (home-owned tablets/laptops, and children's personal mobile phones) will be checked **at the end of each day** (or as set out in the risk assessment). Checks include:
    - Browsing history (including incognito/private mode – if enabled, this may indicate concealment).
    - Text messages, WhatsApp, Snapchat, Instagram DMs, TikTok messages, and other messaging apps.
    - Recently installed/uninstalled apps.
    - Photo gallery and recently deleted photos.
- Adults will record their checks on the child's **daily summary** on Clear Care, noting any concerns or that no concerns were found.

4.4 Internet Use – Guidance and Boundaries

Home Internet Guidance: Within the first 48 hours of placement, the Keyworker will negotiate a written **Internet Guidance** (a section of the ISP) with the child and their social worker. The guidance sets clear boundaries and expectations, including:

- **Time limits** for internet use (e.g., no screens after 9pm, limiting gaming to 1 hour per day).
- **Permitted and prohibited sites** – e.g., educational sites allowed; social media restricted for under-13s; pornography, self-harm, or violent content blocked.
- **Use of personal devices with SIM cards** – if a child brings such a device, adults must change the device's security features (e.g., enable parental controls, content filters, restrict App Store downloads). The child may be required to hand in the device at night.
- **Netiquette** – clear standards of behaviour online (no bullying, no gossiping, no posting photos of others without consent, no impersonation).
- **Consequences** for unacceptable behaviour – e.g., temporary suspension of internet access (see section 4.5).

Special rules for children under 13:

- Children under 13 will not be allowed to set up accounts on social networking sites (most sites require age 13+ anyway). The home will not give permission for a child under 13 to join such sites.
- If a child under 13 attempts to access social media in breach of the ISP, the home will temporarily suspend access and discuss with the social worker.

Privacy settings: Before a child is given access to the internet, adults must ensure that privacy settings are set appropriately (e.g., location turned off, profile set to private, blocking unknown contacts).

Encouraging reporting: Adults will actively encourage children to let them know if they see content that is inappropriate, or if anyone makes them feel upset or uncomfortable online. This is reinforced in key working sessions.

Review: The Home's Internet Guidance will be reviewed at least monthly in key working sessions, or immediately after any online safety incident.

4.5 Monitoring, Supervision and Encouraging Safe Use

Supervision levels:

- **1:1 supervision** is the default. Adults must sit with the child (or be in visual contact) while they use the internet, unless the risk assessment explicitly permits independent supervised use (e.g., the child is 16+ with good online safety awareness). In such cases, the adult still must check the device after use.
- Staff must not leave a child unattended with a device while the child is known to be at risk of viewing harmful content.

Recording and checking – daily process:

Time	Action
End of day (or as per ISP)	Staff member collects child's devices (including personal mobile).
–	Checks browsing history, messages, photos, app list.
–	Records: "Checked J. Smith's phone – browsing history clear, no concerning messages. Device returned." (or note any incidents).

Temporary suspension of internet use as a consequence:

- If a child is found accessing inappropriate sites or behaving unacceptably online (e.g., cyber-bullying, sending sexual images), the Registered Manager may **temporarily suspend** internet use as a proportionate consequence. This may include removing the device for a set period.
- The suspension must have a **set review date** (within 72 hours) and be recorded in the incident report. The decision to extend or lift the suspension must be reviewed with the child's social worker.
- Any sanction must be proportionate, time-limited, and not deprive the child of education or necessary communication with family (unless that is part of the risk).

Education and empowerment:

- Adults must actively teach children how to use the internet safely through:
    - An online safety course (e.g., CEOP's Thinkuknow, Bee Safe, or similar).
    - Regular key working conversations about online grooming, sharing images, and reporting concerns.
    - Encouraging children to use the **CEOP Report** button on the Thinkuknow website.
- If an adult lacks confidence in this area, they must request further training from the Registered Manager.

4.6 Support and Training for Staff

All staff (including agency) must complete the following before supervising children's internet use:

- **Induction training** on this policy (including staff personal device rules).
- **Annual refresher** on internet safety, updated to reflect changes in law (Online Safety Act 2023) and emerging risks (new apps, AI chatbots, etc.).
- **Safeguarding training** includes a module on keeping children safe online (grooming, sexting, radicalisation, gaming risks).
- **Bite-size team workshops** delivered by the home's internet safety representative or the Regional Manager.
- Staff must **sign** to confirm they have read and understood this policy.

Monthly review of IT equipment: The home's designated representative will carry out a monthly review of all IT equipment used by children and young people, checking for technical faults, missing security patches, and that content filtering is active.

4.7 Protection and Action to be Taken (Safeguarding and Reporting)

Immediate action when a safeguarding concern arises online:

- If a child is being groomed, exposed to pornographic material, or contacted inappropriately via the internet or a mobile phone, staff must:
    1. **Do not confront the child** in a way that destroys evidence. Preserve the device (put in airplane mode, do not delete messages, take screenshots if possible).
    2. **Report immediately** to the Designated Safeguarding Lead (DSL) and follow the Safeguarding Policy.
    3. The DSL will inform the child's social worker and, where appropriate, the local authority MASH.
    4. Report to **CEOP** via the "Report to CEOP" button on the Thinkuknow website (www.ceop.police.uk).
    5. If there is **immediate risk of harm** (e.g., the child is planning to meet a groomer), call 999.

- **Suspected online terrorist or extremist material** – report via GOV.UK: "Report online material promoting terrorism or extremism".
- **Revenge porn / image-based abuse** – support the victim, report to the police (101 or 999) and to the Revenge Porn Helpline (https://revengepornhelpline.org.uk).
- **Sexting (youth produced sexual imagery)** – follow the home's Harmful Sexual Behaviours Policy and the UK Council for Child Internet Safety (UKCCIS) guidance on sexting. Do not view, copy, or share the image. Secure the device and contact the DSL.

Recording: All online safety incidents must be recorded on Clear Care (incident report) and in the child's daily notes.

4.8 Resources for Further Support

Staff and children can access the following resources:

Organisation	Purpose	Contact
CEOP (Child Exploitation and Online Protection)	Report online grooming or sexual abuse; educational resources (Thinkuknow).	www.ceop.police.uk
Thinkuknow	Online safety education for children, parents, and carers.	www.thinkuknow.co.uk
Childnet International	Resources to help children use the internet constructively and safely.	www.childnet.com
NSPCC Net Aware	Expert reviews and safety advice on social networks, apps, and games.	www.net-aware.org.uk

Report Harmful Content	Report bullying, harassment, threats, impersonation, unwanted sexual advances, violent content, self-harm, suicide, and pornography.	https://reportharmfulcontent.com
Safer Internet Centre	E-safety tips, advice, helpline for professionals (0344 381 4772).	www.saferinternet.org.uk
Revenge Porn Helpline	Support for victims of non-consensual sharing of intimate images.	https://revengepornhelpline.org.uk
Professionals Online Safety Helpline (POSH)	Free advice for professionals and volunteers working with children.	www.saferinternet.org.uk/helpline
Parentshield	Child-safe mobile network (parental controls).	https://parentshield.co.uk

5. How the Home Trains its Staff About this Policy

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

Training Element	Frequency	Method / Content
Induction	Upon appointment	Face-to-face training covering: legal framework (Online Safety Act 2023, GDPR), personal device rules (storage, no social media contact, gross misconduct), children's risk assessments (ISP transport and internet sections), 1:1 supervision default, daily checking of devices (history, messages, apps), Home Internet Guidance (boundaries, time limits, sanctions), reporting to CEOP, and the dual-site operation (62 & 66 Deighton Road).
Annual refresher	Every 12 months	Classroom or virtual session covering updates to legislation (SCCIF 2026, KCSIE 2026), emerging risks (new apps, AI, deepfakes), and refresher on reporting pathways.
Online safety education training	At induction and biennially	Training on how to deliver online safety key working sessions, use Thinkuknow resources, and support children to report concerns.
Sexting (harmful sexual behaviours)	Annually	Training on the home's Harmful Sexual Behaviours Policy and UKCCIS sexting guidance.
Prevent duty (online radicalisation)	Annually	Training on recognising signs of online radicalisation, and reporting to Prevent / Channel.

Record keeping	At induction and refresh	Training on documenting daily checks (daily summary), incident reporting, and preserving evidence.

Staff are required to:

- Read and sign this policy annually.
- Complete all mandatory training.
- Never leave a personal device accessible to children.
- Report any breach of this policy by a colleague.

6. Related Policies and Guidance

This policy must be read in conjunction with:

- Safeguarding Policy
- Harmful Sexual Behaviours Policy
- Bullying and Cyber Bullying Policy
- Code of Conduct and Ethics Policy
- Data Protection Policy
- Individual Safety Plans (ISPs) – internet risk assessment section
- Children's Homes (England) Regulations 2015
- Working Together to Safeguard Children 2026
- Social Care Common Inspection Framework (SCCIF) for Children's Homes 2026
- CEOP Thinkuknow resources
- UK Council for Child Internet Safety (UKCCIS) – "Sexting in schools and colleges" (updated)

7. Policy Approval and Review Details

Byram House

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