PANTHER NETWORKS UNIVERSAL DPIA

Authorised Network Security Logging for Safeguarding

The Organisation DPIA Framework for All Provider Types (Seven Settings)

Version 3.0 | January 2026 | inspection-grade framework | British English | Legislatively verified

Default position: The Organisation treats online safeguarding as a core safeguarding responsibility. Where internet access is provided through Panther Networks Internet Security Services (delivered using SADIE), metadata only security logging is enabled by default to support timely safeguarding intervention and proportionate investigation following disclosures or serious risk indicators, unless a completed setting schedule evidences that logging is not necessary or proportionate in that setting.

Legislative verification date: 26 January 2026

Critical Notice to All Providers

Status: The Organisation DPIA framework designed for adoption across multiple regulated settings with setting-specific schedules.

Safeguarding position: The Organisation recognises that online harms are a significant, evidenced risk for children, young people and vulnerable adults in regulated care and education contexts. This DPIA template is designed to help providers evidence lawful, fair and proportionate internet safeguarding controls within their regulatory duties, including the ability to respond to immediate risk and to investigate historical harm following a disclosure, using minimum necessary metadata only.

This document is operationally usable across The Organisation only where each service completes the relevant Setting Schedule and Consultation Record and obtains governance sign-off.

This document does not authorise routine monitoring of individuals, surveillance of communications, or punitive use of internet activity records.

If a service cannot evidence necessity and proportionality within its setting schedule, logging must not be implemented in that service.

This DPIA is written to withstand inspection, ICO investigation, and legal scrutiny, including Article 8 proportionality tests.

Applicable to Seven Settings:

- Children's Homes (Residential Care)
- Supported Accommodation (16–17 semi-independent)
- Foster Care Services
- CQC-Regulated Providers (Health and Social Care)
- Education Settings (Schools, Colleges, Universities)
- Community Settings (Youth Services, Charities)
- Health Settings (NHS and Private Healthcare)

Document Control and Key Definitions

Document Control Information

Document Type: The Organisation DPIA Framework (Seven Settings)

Publication version: v3.5

Publication date: 10 February 2026

Controller: The Organisation

Processor: Panther Networks (delivering Panther Networks Internet Security Services using SADIE)

OSQA: individual profiles and trauma-informed engagement

Processing Activity: Network security logging (metadata only) to support safeguarding and cybersecurity

Document Reference: PROVIDER-GROUP-DPIA-NETLOG-2026-v3.0

Version: 3.0

Issued: January 2026

Verified Current As Of: 26 January 2026

Review Frequency: Annual or upon material change

Controller and Processor Clarity

The Organisation: the regulated setting or provider that determines why and how internet access is provided for its service users and therefore acts as the data controller for this processing.

Panther Networks: the service provider delivering internet connectivity and security services to The Organisation. Panther Networks implements SADIE controls under contract and acts as a processor where it processes personal data on behalf of The Organisation.

SADIE: the Panther Networks technology used to deliver secure internet access and cybersecurity, including filtering, threat prevention, and metadata only security logging where justified.

OSQA: the platform that enables individual internet connections and profiles and supports safe online and offline trauma-informed interactions, helping services engage people in positive, safe activities and evidence interventions and outcomes.

Setting Specific Nuances (Seven Settings)

The Organisation operates across seven settings. Proportionality differs by environment. This section sets the default posture for each setting and the conditions under which logging may be justified.

Children's Homes (Residential Care)

Regulatory framework: Children's Homes (England) Regulations 2015 (SI 2015/541).

Inspection / oversight regime: Ofsted social care inspection (current framework at inspection date).

Nuance statement: Logging should be exceptional, developmentally informed, and never a substitute for relationship based safeguarding.

Critical considerations: Age range requires developmental proportionality; what may be appropriate for 16–17 is rarely proportionate for younger children. Default position: use filtering and education first; logging requires explicit justification in the setting schedule. Any access must be incident led, time limited, and recorded, with governance oversight.

Supported Accommodation (16–17 semi independent)

Regulatory framework: Supported Accommodation (England) Regulations 2023 (SI 2023/416).

Inspection / oversight regime: Ofsted supported accommodation inspection and monitoring.

Nuance statement: Balance protection with autonomy, dignity, and participation. Bedrooms are private spaces and must be respected.

Critical considerations: Meaningful consultation is required and must be recorded. Access thresholds must reflect higher privacy expectations than residential children's homes. Logging must not infantilise; it must be explained as a protective system, not control.

Foster Care Services

Regulatory framework: Fostering Services (England) Regulations 2011 (SI 2011/581) and National Minimum Standards (2011).

Inspection / oversight regime: Ofsted fostering service inspection.

Nuance statement: Logging is strongly discouraged in family homes; it is rarely proportionate and introduces complex rights issues.

Critical considerations: Multiple household members are data subjects; controller responsibilities become complex. Normalisation principle is central; most households do not log internet behaviour. Default recommendation: do not implement logging in foster homes; use filtering, safer caring discussions, and education.

CQC Regulated Providers (Health and Social Care)

Regulatory framework: Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 (SI 2014/2936).

Inspection / oversight regime: CQC inspection under quality and safety governance expectations.

Nuance statement: Safeguards must protect dignity and decision making, particularly where sensitive inference risk is higher.

Critical considerations: Consider Mental Capacity Act 2005 where relevant; apply decision specific capacity processes. Increase oversight where browsing patterns might reveal sensitive health matters. Ensure governance evidence meets expectations for audit and good governance.

Education Settings

Regulatory framework: Education Act 2002 s175; Education (Independent School Standards) Regulations 2014 (SI 2014/3283); KCSIE (current edition).

Inspection / oversight regime: Ofsted education inspection or equivalent sector oversight.

Nuance statement: Avoid chilling legitimate learning and support seeking. Proportionality varies sharply by age and device model.

Critical considerations: Differentiate school owned devices and BYOD; set expectations clearly. Monitoring must be appropriate and proportionate; staff training is essential. Residential education contexts require strengthened safeguarding justification.

Community Settings (Youth Services, Charities)

Regulatory framework: Working Together to Safeguard Children 2023; data protection law; commissioning requirements.

Inspection / oversight regime: Funder audits and contract monitoring (variable).

Nuance statement: Necessity threshold is higher where WiFi is an amenity; prioritise consent based approaches where appropriate.

Critical considerations: Provide opt out routes and alternatives where possible. Maintain relationship based safeguarding and inclusive practise. Avoid turning community spaces into surveillance environments.

Health Settings (NHS and Private Healthcare)

Regulatory framework: Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 where applicable; confidentiality principles.

Inspection / oversight regime: CQC inspection and NHS contract governance.

Nuance statement: Highest privacy bar. Logging should be exceptional with enhanced oversight to protect therapeutic trust.

Critical considerations: Tighten access scope to the minimum necessary; avoid user focused review unless strictly required. Strengthen governance sign off and review frequency. Ensure explanations protect trust and do not disrupt care relationships.

Executive Summary and Technical Scope

1.1 Purpose

This The Organisation DPIA establishes a lawful, fair, and proportionate framework for limited network security logging to support safeguarding and cybersecurity across multiple regulated settings. It sets out minimum standards and the required setting schedules that must be completed before implementation in any service.

1.2 Core Assurance Statements

Logging is passive and retrospective. It is not live monitoring.

Online safeguarding is treated as a core safeguarding duty in regulated settings and is addressed through proportionate, evidence-based controls.

Metadata only is recorded. No content, messages, searches, or passwords are captured.

Logs are not routinely accessed. Access is strictly trigger-based and authorised by senior management.

Retention is limited to 30 days, then automatic deletion.

Controls exist to protect people from online harms including AI-generated scams, fake content, online abuse, and cyber attacks, and to prevent harmful traffic that reduces internet quality.

1.3 Limitations

This framework must not be treated as a substitute for service-level due diligence. Each service must complete the relevant Setting Schedule and Consultation Record. **Where the proportionality threshold is not met, logging must not be implemented in that service.**

Description of Network Security Logging and Technical Scope

What is Logged (Metadata Only)

- Website domain (for example, instagram.com)
- Date and time stamp
- High-level category (for example, social media, malware, adult content, phishing)
- Security event type (for example, blocked request) where available

What is Not Logged

- Content of webpages
- Messages, emails, or private communications
- Search terms
- Usernames or passwords
- Keystrokes or screen activity

Retention and Deletion

Default retention is 30 days, followed by automatic deletion. Any variation must be justified in the setting schedule.

Access Model

Logs are not accessed routinely. Access is trigger-based, authorised by senior management, and fully audited.

Universal Regulatory Context and Legal Basis Framework

Universal Regulatory Context (January 2026)

This DPIA is grounded in data protection law and sector safeguarding duties. Providers must ensure setting schedules cite the applicable framework for each service.

- Data Protection Act 2018 and the UK GDPR (as incorporated into UK law): core principles and accountability.
- UK GDPR Article 35: DPIA requirement for processing likely to result in high risk, particularly affecting vulnerable individuals.
- Human Rights Act 1998: Article 8 ECHR proportionality and necessity tests.
- Online Safety Act 2023: contemporary online harms context for protective system design.

Legal Basis Framework (The Organisation)

UK GDPR Article 6 Lawful Bases

Primary lawful basis: Article 6(1)(f) legitimate interests (safeguarding and cyber security). Each service must complete a balancing assessment within the setting schedule.

Secondary lawful basis where applicable: Article 6(1)(c) legal obligation (sector protection duties). Services must not claim logging is legally mandated unless explicitly supported by their regulation.

Special Category Data and Inference Risk

Special category data is not intentionally processed. The Organisation **recognises** potential inference risk and mitigates this through **minimisation** and strict access controls.

Necessity and Proportionality Principles

Necessity

Logging may be necessary to reconstruct serious safeguarding incidents or cyber incidents affecting safety or service integrity. Where filtering and relationship-based **practise** can achieve the safeguarding aim without logging, logging should not be implemented.

Proportionality

Proportionality is achieved through metadata only, short retention, trigger-based access, senior **authorisation**, audit trails, and transparent explanation.

Alternatives Considered

- Filtering without logs
- Shorter or longer retention periods
- Education and relationship-based **practise**
- Device policies and safe use agreements

Internet Related Harms and Risk Context

Modern online risks inform the safeguarding rationale for protective network controls.

AI Generated Scams and Impersonation

Sophisticated artificial intelligence tools can create convincing fake profiles, deepfake videos, and impersonation attempts that target vulnerable individuals with unprecedented realism.

Fake Content and Misinformation

Deliberately misleading content spreads rapidly online, potentially causing confusion, distress, or harmful decision making, particularly for those with limited digital literacy.

Online Abuse and Harassment

Cyberbullying, harassment, and abusive communications can have severe impacts on mental health and wellbeing, especially for children and vulnerable adults.

Cyber Attacks Including Phishing and Malware

Malicious actors use phishing emails, malware downloads, and other attack vectors to steal personal information, compromise accounts, and disrupt services.

Exploitation Risks Including Grooming

Online grooming and exploitation represent serious safeguarding risks, with perpetrators using digital platforms to build trust and manipulate vulnerable individuals.

Malicious Traffic That Slows WiFi

Harmful network traffic from malware, botnets, and other malicious sources can significantly degrade internet quality and performance for all residents and service users.

Privacy Invasion & Data Breaches

Unauthorised access to personal data, identity theft, and privacy violations pose significant threats, leading to financial loss, reputational damage, and emotional distress.

Harmful & Illegal Content Exposure

Exposure to content depicting self harm, violence, hate speech, or illegal activities can traumatise individuals and normalise dangerous behaviours, especially among younger users.

Digital Addiction & Excessive Screen Time

Over reliance on digital devices and platforms can lead to addiction, affecting mental health, physical well-being, and social development, particularly in children and adolescents.

Risk Assessment and Core Safeguards Framework

Risk Assessment (Universal)

Services must refine likelihood and impact in their setting schedule.

Risk	Likelihood	Impact	Core Mitigation
Unauthorised access	Low	High	RBAC, authentication, audit trail, encryption where supported
Staff misuse	Low	High	Senior authorisation, form completion, oversight review
Chilling effect	Medium	High	Transparency, education, access only when necessary
Sensitive inference	Medium	Medium	Minimisation, scope restriction, no routine access
Breach	Low	High	Security controls, incident response, retention limits
Loss of trust	Medium	Medium	Youth-centred explanation, participation, consistent practice

Core Safeguards Framework

Technical Safeguards

- metadata only logging
- Secure configuration and patching
- Encryption where supported
- role-based access controls
- Automatic deletion at 30 days

Procedural Safeguards

- trigger-based access only
- Registered Manager authorisation
- Mandatory access form
- Audit trail and oversight
- Staff training and supervision

Oversight Safeguards

- Quarterly governance review of access events
- Annual DPIA review
- Young people/service user feedback loop

Rights, Participation, and Implementation Requirements

Rights, Participation, and Non-Oppressive Practice

This The Organisation commits to a rights-respecting approach. Controls must be explained in a way that avoids marginalisation, shame, or oppression.

Privacy and Dignity

Protected through minimisation and strict access thresholds.

Participation

Meaningful and recorded through consultation.

Complaints

Can be raised without negative consequences.

Practice Language

Must avoid surveillance framing; the purpose is safety and reliability.

Transparency Outputs (Privacy Notices, Easy Read, Posters)

Each service must provide a privacy notice and accessible explanations.

- Service privacy notice including logging purpose, scope, retention, and rights.
- Young person/service user one page explanation.
- Staff guidance note on explaining the policy.
- Communal poster summary where appropriate.

Implementation Requirements (Setting Schedules)

Before implementation, complete Appendix B and Appendix C and obtain governance sign-off.

Log Access Authorisation and Audit Procedure

All access requires Registered Manager authorisation, a completed form, and governance oversight review.

Breach Management and Incident Governance

Any suspected breach must be escalated and assessed for notification obligations under UK GDPR.

Training, Supervision, and Quality Assurance

Staff must be trained in digital safeguarding, trauma-informed communication, and rights-respecting practice.

Review Schedule and Continuous Improvement

Review annually or sooner if risk profile, technology, guidance, or regulation changes.

Appendices and Practice Examples

GLOSSARY

Glossary

Network security logging: Automated technical records limited to metadata.

Metadata: Information about a connection event, not the content.

Trigger-based access: Access only when a defined serious safeguarding or cyber incident trigger is met.

Proportionality: Using the least intrusive measure that can achieve the safeguarding aim.

REFERENCES

Example References (Legislation and Guidance)

- Data Protection Act 2018.
- UK GDPR (as incorporated into UK law), including Article 35.
- Human Rights Act 1998 (Article 8 ECHR).
- Children's Homes (England) Regulations 2015 (SI 2015/541).
- Supported Accommodation (England) Regulations 2023 (SI 2023/416).
- Fostering Services (England) Regulations 2011 (SI 2011/581) and National Minimum Standards (2011).
- Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 (SI 2014/2936).
- Education Act 2002 s175; Education (Independent School Standards) Regulations 2014 (SI 2014/3283).
- Working Together to Safeguard Children 2023 and Following Updates.
- Keeping Children Safe in Education (current edition effective 1 September 2025).
- Online Safety Act 2023.

PRACTICE EXAMPLES

Practice Examples (SADIE and OSQA by Setting)

Children's Homes (Residential Care)

A child reports repeated contact from a fake profile. Staff record the concern and use OSQA to create time-based internet access relationship-based digital safety work. SADIE blocks malicious domains and strengthens phishing protection. A Registered Manager authorises a time-limited metadata review to evidence domains and dates, then records actions and outcomes.

Supported Accommodation (16 to 17)

A young person discloses online coercion linked to an AI-generated scam. SADIE strengthens filtering and blocks known scam domains while keeping support sites accessible. If necessary, a short authorised metadata review confirms domains and timestamps to inform safeguarding decisions and supervision records.

Foster Care Services

In a foster home, the default is no logging. OSQA creates safer caring discussions, boundaries and digital resilience coaching. If an exceptional safeguarding trigger arises, The Organisation uses SADIE on a dedicated network for the foster child, with legal review and clear transparency. Any metadata review is time-limited, minimal, audited and governance reviewed.

CQC Regulated Providers (Health and Social Care)

A service user is targeted by a phishing link and loses account access. Staff document the incident and use OSQA to create online safety activities and update the safeguarding plan, including capacity considerations where relevant. SADIE blocks malicious domains and prevents malware downloads, stabilising network performance. An authorised metadata review confirms domains and times to support protective actions, reporting and learning.

Education Settings

A student receives harmful content links through a messaging app. Staff record the concern and create learning responses in OSQA. SADIE applies age-appropriate filtering, safe search and anti-malware protection on the school network. Where the school controls the network, an authorised metadata review confirms domains and timestamps to inform pastoral support, parent liaison and safeguarding escalation.

Community Settings (Youth Services, Charities)

A young person using a youth hub device reports harassment and a malicious link. OSQA creates resources for teaching the principles of consent, boundaries and scam spotting. SADIE blocks the harmful domain and reduces malicious traffic that slows connectivity for everyone. Logging remains minimal and is accessed only where a serious safeguarding trigger is met and authorised.

Health Settings (NHS and Private Healthcare)

A clinic experiences repeated phishing attempts that risk service disruption. The Organisation uses SADIE to block malicious domains and protect accounts, reducing harmful traffic that degrades network quality. OSQA provides staff with learning for governance. If safeguarding risk emerges, a senior authorised, time-limited metadata review supports safe intervention using minimum necessary data only.