



STARFISH AP
The Starfish Way
Online Safety & Digital Technology Policy
Academic Year: 2026–2027

Document Title	Online Safety & Digital Technology Policy
Organisation	Starfish Alternative Provision
Academic Year	2026–2027
Version	1
Policy Owner	Chloe Fox –
Designated Safeguarding Lead (DSL)	Chloe Fox
Applies To	All employees, volunteers, agency staff, contractors,
Date Approved	Sep 2026
Review Date	Sep 2027
Next Review	Annually, or sooner following legislative or statutory

Document Purpose

This policy sets out The Starfish Hub's commitment to creating a safe, secure and responsible digital environment that supports learning, safeguards children and promotes positive digital citizenship.

Technology plays an important role in modern education, communication and everyday life. Alongside its many benefits, digital technology also presents evolving safeguarding, privacy and security risks. The Starfish Hub is committed to ensuring that children, staff and visitors are equipped to use technology safely, responsibly and confidently.

Our approach extends beyond filtering inappropriate content. We aim to develop a culture where online safety is understood as a shared responsibility, underpinned by education, professional accountability and strong safeguarding practice.

This policy outlines how The Starfish Hub manages technology, protects children and staff online, promotes responsible digital behaviour, responds to online safety concerns and works in partnership with families, commissioning schools, Local Authorities and our specialist IT providers to maintain secure digital systems.

The Starfish Hub recognises the rapidly changing nature of technology, including developments in artificial intelligence (AI), social media and digital communication. We are committed to regularly reviewing our practice to ensure that our online safety arrangements remain effective, proportionate and responsive to emerging risks.

This policy should be read alongside The Starfish Hub's Safeguarding & Child Protection Policy, Staff Code of Conduct, Behaviour, Relationships & Relational Practice Policy and the wider policies forming part of The Starfish Way Governance & Practice Framework.

The Starfish Way

At The Starfish Hub, we believe that safeguarding extends beyond our physical environment into every digital space that children and adults access.

Technology provides valuable opportunities to learn, communicate and connect with others. It also brings new responsibilities to protect privacy, maintain professional boundaries and ensure that children can navigate the online world safely and confidently. Many of the children attending The Starfish Hub have experienced vulnerability, disruption or adversity. We recognise that these experiences may increase the risks associated with online exploitation, cyberbullying, harmful content or unsafe digital relationships.

Our role is not simply to block inappropriate content.

Our role is to equip children with the knowledge, confidence and critical thinking skills needed to become safe, respectful and responsible digital citizens. We believe that online safety is achieved through education, trusted relationships, secure systems and a shared commitment to safeguarding.

The Starfish Way is built upon eight guiding principles:

- **Safety** – Every child has the right to feel safe both offline and online.
- **Trust** – Digital technologies should strengthen relationships whilst maintaining clear professional boundaries.
- **Attunement** – We remain aware of emerging digital risks and respond proactively to protect children and staff.
- **Regulation** – We encourage healthy, balanced and responsible use of technology that supports wellbeing.
- **Flexibility** – We continually review and adapt our digital practices as technology evolves.
- **Inclusion** – Every child should be able to access technology safely and equitably, with appropriate support where needed.
- **Support** – We work collaboratively with families, commissioning schools, Local Authorities and specialist partners to promote online safety.
- **Humanity** – Every digital interaction should reflect kindness, professionalism, respect and integrity.

These principles underpin every decision we make regarding technology and digital safeguarding. At The Starfish Hub, online safety is not simply about preventing harm. It is about empowering children to use technology confidently, responsibly and safely throughout their lives.

Contents

1. Online Safety Culture
2. Roles and Responsibilities
3. Technology Infrastructure
4. Filtering and Monitoring
5. Acceptable Use of Technology
6. Staff Devices and Professional Boundaries
7. Children and Digital Citizenship
8. Photography, Images and Social Media
9. Artificial Intelligence (AI)
10. Cyber Security and Data Protection
11. Responding to Online Safety Concerns
12. Monitoring, Review and Quality Assurance
13. Related Policies
14. The Starfish Commitment
15. Appendices

Online Safety Culture

At The Starfish Hub, online safety is recognised as an integral part of safeguarding and forms part of our wider commitment to promoting the safety, wellbeing and rights of every child. We believe that creating a safe digital environment extends beyond filtering inappropriate content or restricting access to technology. It is achieved through education, trusted relationships, professional accountability and a culture in which children and adults understand how to use technology safely, respectfully and responsibly.

Online safety is embedded throughout the curriculum, daily practice and wider life of the provision.

Staff actively promote:

- safe and responsible use of technology
- respectful online communication
- critical thinking when accessing online content
- awareness of online risks
- healthy digital habits
- appropriate professional boundaries
- responsible use of Artificial Intelligence (AI).

Children are encouraged to speak openly with trusted adults about anything they encounter online that makes them feel worried, uncomfortable or unsafe.

All online safety concerns are treated seriously and managed in accordance with The Starfish Hub's Safeguarding & Child Protection Policy.

Roles and Responsibilities

Maintaining a safe digital environment is a shared responsibility. Every member of the Starfish community has a role in promoting safe, responsible and respectful use of technology.

The Director & Designated Safeguarding Lead will:

- oversee the implementation of this policy
- ensure online safety remains a safeguarding priority
- respond appropriately to online safety concerns
- ensure staff receive appropriate training
- review filtering and monitoring arrangements regularly
- work collaboratively with Harrap ICT and Senso to maintain safe digital systems

- ensure incidents are recorded on CPOMS where appropriate
- review emerging risks and update procedures accordingly.

All Staff will:

- model safe and professional use of technology
- maintain professional boundaries at all times
- follow The Starfish Hub's acceptable use expectations
- remain alert to signs of online abuse, exploitation or cyberbullying
- report concerns immediately
- complete online safety training as part of induction and ongoing professional development
- promote positive digital citizenship through everyday interactions.

Children and Young People will be encouraged to:

- use technology safely and responsibly
- respect others when communicating online
- protect their own personal information
- report anything online that makes them feel unsafe
- ask for help whenever they are unsure.

Parents and Carers are encouraged to:

- work in partnership with The Starfish Hub to promote safe technology use
- discuss online safety regularly with their child
- report concerns that may affect a child's wellbeing
- support healthy and balanced use of technology at home.

Technology Infrastructure

The Starfish Hub is committed to maintaining secure, reliable and appropriately managed technology systems that support learning whilst safeguarding children and staff.

The provision's IT infrastructure is managed in partnership with Harrap ICT, who provide installation, maintenance and ongoing technical support for The Starfish Hub's technology systems.

Harrap ICT work collaboratively with The Starfish Hub to:

- maintain secure digital infrastructure
- implement appropriate cyber security measures
- undertake routine maintenance
- support the management of staff and student devices
- advise on emerging digital risks
- conduct regular audits of systems and practice to support compliance with Department for Education expectations and recognised cyber security standards.

These arrangements help ensure that The Starfish Hub's digital environment remains secure, reliable and fit for purpose.

Filtering and Monitoring

The Starfish Hub recognises that effective filtering and monitoring systems are essential components of safeguarding. In accordance with Keeping Children Safe in Education and the Department for Education's Filtering and Monitoring Standards, appropriate systems are in place to reduce the risk of children accessing harmful or inappropriate content and to identify potential safeguarding concerns.

Filtering and monitoring services are provided through Senso.

These systems apply to:

- devices owned and managed by The Starfish Hub
- staff devices provided for professional use
- student devices provided by The Starfish Hub
- devices connected to The Starfish Hub's wireless network, where appropriate.

Filtering and monitoring support the identification of:

- inappropriate online content
- attempts to bypass filtering systems
- concerning searches
- indicators of online exploitation
- cyberbullying
- inappropriate use of technology
- other safeguarding concerns.

Filtering and monitoring systems are intended to support safeguarding and do not replace professional vigilance.

All concerns identified through these systems will be reviewed appropriately and, where necessary, managed in accordance with The Starfish Hub's Safeguarding & Child Protection Policy.

Filtering and monitoring arrangements are reviewed regularly in partnership with Harrap ICT to ensure they remain effective, proportionate and responsive to emerging risks.

The Starfish Reflection

Technology should create opportunities, not risks.

At The Starfish Hub, we believe that safeguarding children online is achieved through secure systems, knowledgeable adults and confident young people who know that they can always seek help when something does not feel right.

Acceptable Use of Technology

Technology is an important part of teaching, learning, communication and safeguarding at The Starfish Hub. All members of the Starfish community are expected to use technology responsibly, respectfully and in ways that protect both themselves and others. Technology must always be used in a manner that reflects The Starfish Way and supports the safety, wellbeing and dignity of every member of our community.

All users of technology are expected to:

- use technology safely and responsibly
- respect the privacy of others
- protect confidential information
- use technology only for appropriate educational or professional purposes
- report any concerns immediately to a trusted adult or the Designated Safeguarding Lead
- follow the guidance contained within this policy and all associated procedures.

The Starfish Hub reserves the right to investigate any misuse of technology where this is necessary to safeguard children, protect staff or maintain the security of organisational systems.

Staff Devices and Professional Boundaries

The Starfish Hub is committed to maintaining clear professional boundaries and protecting both children and staff through safe and secure use of technology. Where possible, staff should use technology and devices provided or approved by The Starfish Hub for all work-related activities.

Staff should not use personal devices for work purposes where organisational equipment or systems are available.

Where authorised, staff may access approved organisational systems using a personal device. This must only be for legitimate work purposes and must not involve downloading, storing or sharing confidential information outside approved secure systems.

Staff are expected to ensure that any authorised personal device used for work purposes is appropriately secured through password protection and appropriate security settings.

Professional Communication

Professional boundaries are essential to safeguarding.

Staff must never:

- provide children or families with their personal mobile telephone number
- provide personal email addresses
- communicate with children through personal social media accounts
- use personal messaging applications for professional communication with children or families
- accept or initiate social media connections with current pupils.

All communication with children, parents/carers, commissioning schools and professionals must take place using approved organisational systems and contact methods.

Maintaining appropriate professional boundaries protects children, families and staff and reduces the risk of misunderstandings, allegations or breaches of professional conduct.

Photography, Images and Social Media

The Starfish Hub is committed to protecting the identity, privacy and dignity of every child. As part of our safeguarding commitment, identifiable photographs or videos of children and young people attending The Starfish Hub will not be published on social media platforms, our website or within marketing materials.

This reflects our commitment to protecting children from the increasing risks associated with the online misuse of images, including unauthorised sharing, image manipulation through Artificial Intelligence (AI), deepfake technology and other forms of digital exploitation.

Where photographs are used to celebrate learning or promote the work of The Starfish Hub, they will:

- avoid identifying individual children
- protect children's identities through careful composition where appropriate
- only be used where appropriate permissions have been obtained
- always prioritise safeguarding over publicity.

The Starfish Hub believes that children's right to privacy and protection should always take precedence over marketing or promotional activity.

Social Media

The Starfish Hub's official social media platforms are used to celebrate learning, share information with our community and communicate professionally with families and partner organisations.

All content published on behalf of The Starfish Hub must:

- reflect the values of The Starfish Way
- maintain confidentiality
- protect children's identities
- be accurate, respectful and professional
- comply with safeguarding and data protection requirements.

Where staff respond to messages or enquiries through The Starfish Hub's official social media accounts, responses will be signed off using the staff member's first name or agreed professional identifier, making it clear that they are communicating in their professional capacity on behalf of The Starfish Hub.

Staff must never use personal social media accounts to conduct Starfish Hub business.

Artificial Intelligence (AI)

The Starfish Hub recognises that Artificial Intelligence (AI) is becoming an increasingly important part of education and wider society.

AI has the potential to enhance learning, improve efficiency and support creativity when used safely, ethically and responsibly.

Staff may use approved AI tools to support professional activities such as lesson planning, resource creation and administrative tasks.

However, AI must never replace professional judgement.

Staff must not:

- enter confidential or personally identifiable information into publicly available AI platforms
- use AI to make safeguarding decisions
- rely upon AI-generated content without checking its accuracy
- use AI to write safeguarding records or professional reports without appropriate review and professional oversight.

Children will be supported to develop an age-appropriate understanding of AI, including:

- how AI works
- its benefits and limitations
- recognising misinformation
- protecting personal information
- understanding that AI-generated content is not always accurate or reliable
- using AI safely, ethically and responsibly.

The Starfish Hub will continue to review its use of AI in response to developments in technology, legislation and national guidance.

The Starfish Reflection

Technology should strengthen relationships, protect dignity and expand opportunity; never compromise safety or trust.

At The Starfish Hub, we embrace technology with curiosity and ambition, whilst recognising that safeguarding, professional judgement and human relationships must always remain at the centre of our practice.

Cyber Security and Data Protection

The Starfish Hub recognises that effective cyber security is an essential aspect of safeguarding, protecting sensitive information and maintaining the integrity of our digital systems. All staff have a responsibility to protect organisational systems, confidential information and personal data from unauthorised access, misuse or loss.

Staff are expected to:

- use strong and secure passwords
- keep passwords confidential and never share them with others
- lock devices when unattended
- report suspected phishing emails, scams or cyber security concerns immediately
- ensure software updates are completed promptly where required
- store confidential information only within approved organisational systems
- follow The Starfish Hub's Data Protection & Confidentiality Policy at all times.

Any actual or suspected data breach will be managed in accordance with The Starfish Hub's Data Protection procedures and, where appropriate, reported to relevant authorities in line with UK GDPR and Data Protection Act 2018 requirements. The Starfish Hub works alongside Harrap ICT to maintain secure systems, implement appropriate cyber security measures and respond promptly to emerging digital threats.

Responding to Online Safety Concerns

Online safety concerns are treated as safeguarding concerns whenever there is a risk that a child or young person may be experiencing harm.

Concerns may include, but are not limited to:

- cyberbullying
- online grooming
- child sexual exploitation
- child criminal exploitation
- sharing of indecent images
- sextortion
- online coercion or manipulation
- exposure to harmful or inappropriate content
- extremist or radicalising material
- online abuse
- concerning online searches
- misuse of Artificial Intelligence (AI)
- inappropriate use of technology by children or adults.

All members of staff have a duty to act immediately if they become aware of an online safety concern.

Staff will:

- reassure the child and listen without judgement
- avoid investigating beyond what is necessary to establish the concern
- preserve evidence where appropriate
- report concerns immediately to the Designated Safeguarding Lead
- record concerns on CPOMS before the end of the working day, or as soon as reasonably practicable
- follow The Starfish Hub's Safeguarding & Child Protection Policy.

Where appropriate, concerns may be shared with:

- parents or carers
- commissioning schools
- Local Authorities
- Children's Services
- the Police
- other relevant safeguarding agencies.

The welfare of the child will always remain the primary consideration when determining the most appropriate response.

Staff Training and Professional Development

The Starfish Hub recognises that technology and online risks evolve rapidly. To ensure children remain protected, all staff receive regular training appropriate to their role and responsibilities.

As a minimum, staff will receive training in:

- online safety and digital safeguarding
- recognising indicators of online abuse and exploitation
- cyber security awareness
- data protection and confidentiality
- acceptable use of technology
- professional boundaries
- Artificial Intelligence (AI) awareness and safe use
- filtering and monitoring systems
- reporting online safety concerns.

Training forms part of staff induction and is refreshed regularly to reflect changes in legislation, technology and emerging safeguarding risks.

Where appropriate, additional guidance or specialist training will be provided in response to local or national safeguarding concerns.

Monitoring, Review and Quality Assurance

The Starfish Hub is committed to maintaining the highest standards of digital safeguarding. The Director & Head of Provision, supported by Harrap ICT and our filtering and monitoring provider, Senso, will regularly review:

- filtering and monitoring arrangements
- cyber security measures
- online safety incidents
- safeguarding concerns relating to technology
- staff compliance with this policy
- developments in technology and Artificial Intelligence
- Department for Education guidance
- recommendations arising from safeguarding reviews or audits.

Regular audits of the provision's technology systems will be undertaken in partnership with Harrap ICT to ensure that digital safeguarding arrangements continue to meet Department for Education expectations and recognised good practice.

Findings from monitoring and quality assurance activities will be used to strengthen practice, identify training needs and continually improve The Starfish Hub's digital safeguarding arrangements.

Related Policies

This policy should be read alongside:

- Safeguarding & Child Protection Policy
- Behaviour, Relationships & Relational Practice Policy
- Attendance, Engagement & Belonging Policy
- Positive Handling, Physical Intervention & De-escalation Policy
- SEND & Inclusion Policy
- Staff Code of Conduct
- Data Protection & Confidentiality Policy
- Health & Safety Policy
- First Aid & Administration of Medication Policy

The Starfish Commitment

At The Starfish Hub, we believe that safeguarding does not end at the classroom door. Children deserve to feel safe wherever they learn, communicate and connect—including online. Technology should be a tool that opens doors, broadens opportunities and strengthens relationships, never one that compromises safety, dignity or wellbeing.

We are committed to creating a digital culture where children learn to navigate the online world with confidence, curiosity and critical thinking, supported by adults who model professionalism, integrity and responsible use of technology.

By combining robust safeguarding systems, secure technology, ongoing education and strong partnerships with families, commissioning schools and specialist providers, we strive to create an environment where every child can benefit from technology safely and responsibly.

At The Starfish Hub, digital safeguarding is not simply about protecting children from harm.

It is about empowering them to thrive safely in an increasingly connected world. Every child. Every click. Every opportunity.

Appendix A – The Starfish Digital Safety Framework

1. Educate

We teach children how to use technology safely, responsibly and confidently.



2. Protect

Secure systems, filtering, monitoring and professional boundaries reduce digital risk.



3. Recognise

Staff remain vigilant to signs of online abuse, exploitation, cyberbullying and emerging digital harms.



4. Respond

Concerns are reported immediately, recorded on CPOMS and managed in line with safeguarding procedures.



5. Reflect

Incidents are reviewed to identify learning, strengthen systems and continually improve practice.



6. Grow

Children develop the knowledge, resilience and digital citizenship skills needed to navigate an ever-changing online world safely.