



STARFISH AP
The Starfish Way
Data Protection & Information Governance Policy
Academic Year 2026–2027

Document Title	Data Protection & Information Governance Policy
Organisation	Starfish Alternative Provision
Academic Year	2026–2027
Version	1
Policy Owner	Chloe Fox – Director & Head of Provision
Data Protection Officer (DPO)	Chloe Fox – Director & Head of Provision
Applies To	All employees, volunteers, agency staff, contractors, pupils, parents/carers, commissioning schools, Local Authorities and professionals working with or on behalf of The Starfish Hub
Date Approved	Sep 2026
Review Date	Sep 2027

Document Purpose

This policy sets out The Starfish Hub's approach to data protection, confidentiality, information governance and the lawful processing of personal information.

At The Starfish Hub, we recognise that children, families, commissioning schools, Local Authorities, professionals and staff place significant trust in us. That trust extends not only to the care, education and support we provide, but also to how we handle the personal information they share with us.

We are committed to ensuring that all personal information is collected, processed, stored, shared and disposed of lawfully, fairly, transparently and securely. Effective information governance supports safeguarding, protects privacy, strengthens professional accountability and helps ensure that children receive the right support at the right time.

This policy outlines how The Starfish Hub manages personal information, protects confidentiality, responds to data breaches, shares information appropriately and complies with data protection legislation.

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

The Starfish Way

At The Starfish Hub, trust sits at the heart of every relationship.

Children, families, commissioning schools and professionals share personal information with us because they trust that it will be handled with care, dignity and respect. Protecting information is therefore not simply an administrative task or legal requirement. It is a safeguarding responsibility and an essential part of professional practice.

Many of the children attending The Starfish Hub have experienced adversity, disrupted education, trauma or complex life experiences. Effective support often relies upon professionals sharing information appropriately, accurately and securely.

The Starfish Way is built upon eight guiding principles:

Safety

Protecting personal information helps safeguard children and adults from harm.

Trust

Trust grows when information is handled responsibly and transparently.

Attunement

We seek to understand individual circumstances and information-sharing needs.

Regulation

Clear systems and procedures help ensure safe, consistent decision-making.

Flexibility

We respond proportionately to differing circumstances whilst maintaining compliance.

Inclusion

Information should be accessible, understandable and available to those who need it.

Support

Effective information sharing enables collaborative support for children and families.

Humanity

Every piece of information represents a real person whose dignity and rights deserve protection.

When considering information governance, we do not simply ask:
"Can we share this information?"

We also ask:

"Should this information be shared, who needs to know, how can it be shared safely, and what is in the best interests of the child?"

Scope

This policy applies to:

- All employees.
- Volunteers.
- Agency staff.
- Contractors.
- Consultants.
- Visiting professionals.
- Pupils.
- Parents and carers.
- Commissioning schools.
- Local Authorities.
- Partner agencies.

The policy applies to all personal information held in any format, including:

- Electronic records.
- Emails.
- Cloud-based systems.
- Paper files.
- Assessment records.
- Safeguarding records.
- Photographs.
- Video recordings.
- Communication systems.
- Mobile devices.

Legislative and Regulatory Framework

This policy has been developed in accordance with:

- UK General Data Protection Regulation (UK GDPR).
- Data Protection Act 2018.
- Freedom of Information Act 2000 (where applicable).
- Education (Pupil Information) Regulations.

- Keeping Children Safe in Education (Current Edition).
- Working Together to Safeguard Children (Current Edition).
- Information Commissioner's Office (ICO) guidance.
- Department for Education guidance relating to schools and Alternative Provision.

The Starfish Hub will review this policy whenever legislation, statutory guidance or regulatory expectations change.

Data Protection Principles

The Starfish Hub processes personal information in accordance with the principles of UK GDPR.

Personal information will be:

Lawful, Fair and Transparent

Information will only be processed where there is a lawful basis to do so.

Collected for Legitimate Purposes

Information will only be collected for specified educational, safeguarding, employment or operational purposes.

Adequate and Relevant

Only information that is necessary for a specific purpose will be collected and retained.

Accurate

Reasonable steps will be taken to ensure information remains accurate and up to date.

Retained Appropriately

Information will only be retained for as long as necessary or required by law.

Secure

Appropriate physical, organisational and technical measures will be used to protect information.

Accountable

The Starfish Hub will be able to demonstrate compliance with data protection requirements.

Roles and Responsibilities

Director and Head of Provision / Data Protection Officer

Chloe Fox serves as the Data Protection Officer (DPO) for The Starfish Hub.

The DPO is responsible for:

- Monitoring compliance with data protection legislation.
- Advising staff regarding data protection matters.
- Responding to Subject Access Requests.
- Investigating data breaches.
- Maintaining oversight of information governance arrangements.
- Liaising with external agencies where required.
- Acting as the primary contact for the Information Commissioner's Office (ICO).

All Staff

All staff are responsible for:

- Protecting confidential information.
- Following organisational procedures.
- Using approved systems only.
- Reporting concerns immediately.
- Maintaining professional confidentiality.
- Completing required training.

Staff must never access information unless there is a legitimate professional reason for doing so.

Information We Hold

The Starfish Hub may process information relating to:

Pupils

Including:

- Personal details.
- Attendance information.

- Assessment records.
- SEND information.
- Behaviour records.
- Safeguarding records.
- Medical information.
- Risk assessments.
- Pupil voice information.
- Photographs and educational records.

Parents and Carers

Including:

- Contact details.
- Communication records.
- Consent information.
- Emergency contact details.

Staff

Including:

- Recruitment records.
- Employment information.
- Training records.
- Payroll information.
- Safeguarding declarations.
- Performance management information.

Professionals and Partner Agencies

Including information necessary to support partnership working and safeguarding responsibilities.

Information Systems Used by The Starfish Hub

To support education, safeguarding and operational management, The Starfish Hub uses secure digital systems including:

Arbor

Used for:

- Pupil records.
- Attendance.
- Assessment.
- Communication.
- Operational administration.

CPOMS

Used for:

- Safeguarding records.
- Child protection concerns.
- Wellbeing monitoring.
- Safeguarding chronologies.
- Multi-agency safeguarding information.

Access to safeguarding records is restricted according to role and safeguarding responsibilities.

Senso

Used to support:

- Online monitoring.
- Digital safeguarding.
- Filtering and monitoring requirements.
- Identification of potential online safety concerns.

Monitoring arrangements are implemented to protect children and meet safeguarding responsibilities.

Google Workspace for Education

Used for:

- Email communication.
- Shared documents.
- Educational resources.

- Internal collaboration.
- Secure information storage.

Google Workspace for Education services are managed and supported by Harrap ICT Services in accordance with contractual security and data protection requirements.

Connecteam

Used for:

- Staff communication.
- Scheduling.
- Workforce management.
- Operational updates.
- Internal communication.

Staff are expected to use Connecteam responsibly and in accordance with confidentiality expectations.

Lawful Processing

The Starfish Hub processes personal information only where a lawful basis exists.

This may include:

- Compliance with legal obligations.
- Performance of a public task.
- Contractual obligations.
- Vital interests.
- Legitimate interests where appropriate.
- Consent where required.

Where special category data is processed, an additional lawful condition under relevant legislation will also apply.

Information Sharing and Safeguarding

The Starfish Hub recognises that appropriate information sharing is essential for safeguarding and supporting children effectively.

Information may be shared where:

- There is a lawful basis.

- A safeguarding concern exists.
- There is a statutory duty to share information.
- Consent has been obtained where appropriate.
- Sharing is necessary to protect a child or vulnerable individual.

Information sharing decisions will be:

- Necessary.
- Proportionate.
- Relevant.
- Accurate.
- Timely.
- Securely recorded.

The safety and welfare of children will always remain a primary consideration.

Confidentiality

All staff are expected to maintain professional confidentiality.
Information must only be discussed with individuals who have a legitimate professional need to know.

Staff must not:

- Access records without authorisation.
- Share confidential information in public areas.
- Discuss pupils outside professional contexts.
- Use personal email accounts for organisational business.
- Disclose information without a lawful basis.

Confidentiality obligations continue after employment or engagement with The Starfish Hub ends.

Use of Personal Devices

The Starfish Hub recognises that approved systems, including Connecteam, may be accessed through personal devices.

Staff using personal devices for work purposes must:

- Use secure passwords.
- Maintain device security.
- Enable device locking features.
- Report loss or theft immediately.
- Prevent unauthorised access.
- Avoid storing confidential information outside approved systems.

Where concerns arise regarding information security, staff may be required to cooperate with reasonable investigations relating to organisational data.

Subject Access Requests

Individuals have the right to request access to personal information held about them.

Requests should be directed to the Data Protection Officer.

The Starfish Hub will:

- Verify identity where appropriate.
- Respond within statutory timescales.
- Provide information in an accessible format where possible.
- Apply lawful exemptions where permitted.

Further information is available within The Starfish Hub's Privacy Notices.

Data Breaches

A data breach includes any accidental or unlawful:

- Loss of information.
- Destruction of information.
- Alteration of information.
- Unauthorised disclosure.
- Unauthorised access.

Examples may include:

- Sending information to the wrong recipient.
- Lost devices.
- Unauthorised access to records.
- Cyber-security incidents.
- Loss of paper records.

All actual or suspected breaches must be reported immediately to the Data Protection Officer.

The DPO will:

- Assess the risk.
- Investigate the incident.
- Take corrective action.
- Consider reporting requirements.
- Notify the ICO where legally required.

Record Retention and Secure Disposal

Records will be retained in accordance with statutory requirements and recognised retention schedules.

When information is no longer required it will be:

- Securely deleted.
- Confidentially shredded.
- Permanently destroyed using approved methods.

The Starfish Hub will take reasonable steps to ensure information cannot be recovered once disposed of.

Privacy Notices

The Starfish Hub maintains separate Privacy Notices for relevant stakeholders, including:

- Pupils.
- Parents and carers.
- Staff.
- Volunteers.
- Website users.

These notices explain:

- What information is collected.
- Why it is collected.
- How it is used.
- How long it is retained.
- Who it may be shared with.
- Individual rights regarding personal information.

Privacy Notices are available upon request and via The Starfish Hub website.

Training

All staff will receive appropriate training regarding:

- Data protection.
- Confidentiality.
- Information sharing.
- Safeguarding information management.
- Cyber security awareness.
- Use of organisational systems.

Refresher training will be provided as required.

Monitoring and Review

The Director and Head of Provision will monitor:

- Data breaches.
- Information security incidents.
- Subject Access Requests.
- Training compliance.
- Information sharing practices.
- Emerging risks and technological developments.

Learning from incidents, audits and reviews will be used to strengthen information governance arrangements and improve practice across The Starfish Hub.

This policy will be reviewed annually, or sooner where changes to legislation, technology or organisational practice require amendment.