PERSON RESPONSIBLE FOR POLICY:	***PAUL MILLS***
APPROVED:	***MICHELLE HARVEY***
SIGNED:	***PAUL MILLS***
TO BE REVIEWED:	***SEPTEMBER 2027***

UKPRN: 10101682 | Legal Address: Thistledown Barn, 204 Holcot Lane, Sywell NN6 0BG

SNAP

DATA PROTECTION AND INFORMATION GOVERNANCE POLICY

1. POLICY STATEMENT

SNAP is committed to protecting the personal information of learners, parents/carers, staff, visitors, commissioners, professionals and other individuals with whom it works.

As an Alternative Provision setting, SNAP recognises that it processes personal and sensitive information to support education, safeguarding, attendance, wellbeing, SEND, behaviour, administration and communication with commissioning schools, academies, local authorities and other relevant organisations.

SNAP will comply with applicable data protection legislation, including:

- the UK General Data Protection Regulation (UK GDPR);
- the Data Protection Act 2018, as amended;
- the Data (Use and Access) Act 2025, where applicable;
- the Privacy and Electronic Communications Regulations, where applicable; and
- relevant Information Commissioner's Office (ICO) guidance.

KCSIE 2026 refers collectively to the Data Protection Act 2018, UK GDPR and Data (Use and Access) Act 2025 as the data protection laws.

---

2. DATA PROTECTION RESPONSIBILITY

SNAP will identify an individual with overall responsibility for data protection and information governance.

Where SNAP is legally required to appoint a Data Protection Officer (DPO), it will do so and ensure that the DPO has appropriate independence, expertise and resources.

Where SNAP does not require a statutory DPO, an appropriate person will nevertheless be responsible for overseeing data protection compliance.

Data Protection Lead/DPO: Paul Mills

Contact: 07951286442

---

3. ICO REGISTRATION

SNAP will determine whether it is required to register with the Information Commissioner's Office and pay the applicable data protection fee.

Where SNAP is required to register, it will maintain its registration and pay the applicable fee.

ICO Registration Number: ZC181264

---

4. DATA CONTROLLER, PROCESSOR AND COMMISSIONING ARRANGEMENTS

SNAP will establish whether it is acting as:

- a data controller;

- a joint controller; or
- a data processor

for each significant processing activity.

This is particularly important because SNAP provides Alternative Provision commissioned by schools, academies and/or local authorities.

Where SNAP processes information on behalf of another organisation, appropriate contractual arrangements will establish the responsibilities of each organisation.

Where appropriate, SNAP will have written data-sharing or data-processing arrangements with commissioning organisations and other relevant organisations.

---

5. DATA PROTECTION PRINCIPLES

SNAP will ensure that personal data is:

Lawful, fair and transparent

Personal data will only be processed where there is a valid lawful basis and individuals are provided with appropriate information about how their information is used.

Purpose limited

Information will be collected for specified, explicit and legitimate purposes.

Adequate, relevant and limited

SNAP will only collect information that is necessary for the purpose for which it is being processed.

Accurate

Reasonable steps will be taken to ensure information is accurate and kept up to date where necessary.

Subject to storage limitation

Personal data will not be retained for longer than necessary.

Secure

Personal information will be protected against unauthorised or unlawful processing and accidental loss, destruction or damage.

Accountable

SNAP will be able to demonstrate compliance with its data protection responsibilities.

---

6. LAWFUL BASIS FOR PROCESSING

SNAP will identify and document the appropriate lawful basis before processing personal data.

Depending on the circumstances, this may include:

- legal obligation;
- contract;
- legitimate interests;
- vital interests;
- public task, where applicable; or
- consent.

Consent is not automatically required for all processing or information sharing.

Where SNAP relies on consent, consent must be freely given, specific, informed and capable of being withdrawn.

For safeguarding purposes, SNAP will normally consider whether another lawful basis is more appropriate than consent.

---

7. SPECIAL CATEGORY AND CRIMINAL OFFENCE DATA

SNAP may process information requiring additional protection, including information concerning:

- health;
- disability;
- racial or ethnic origin;
- religious or philosophical beliefs;
- biometric information, where applicable;
- sexual orientation;
- trade union membership; and
- criminal convictions and offences.

Where special category data is processed, SNAP will identify both an appropriate Article 6 lawful basis and an appropriate Article 9 condition.

Where criminal offence data is processed, SNAP will ensure that the appropriate legal requirements and safeguards are met.

Safeguarding information may include sensitive or special category personal data. Staff must understand the relevant processing conditions which allow such information to be shared for safeguarding purposes, including where consent is not required.

Where required, SNAP will maintain an Appropriate Policy Document.

---

8. DATA PROTECTION IMPACT ASSESSMENTS

SNAP will consider whether a Data Protection Impact Assessment (DPIA) is required before introducing processing likely to result in a high risk to individuals.

This may include:

- new technology;
- monitoring systems;
- CCTV;
- biometric systems;
- significant profiling;
- extensive processing of learner information; or
- new systems involving vulnerable learners.

Where a DPIA identifies significant risks, SNAP will take appropriate steps to reduce those risks.

---

9. LEARNER AND CHILDREN'S DATA

SNAP recognises that learners under 18 may require additional protection because of their age, vulnerability or individual circumstances.

SNAP will:

- process children's information fairly and transparently;
- consider the best interests of the child;
- use clear and accessible privacy information;
- support learners to understand how their information is used;
- respect learners' data protection rights;
- consider age, understanding and capacity when responding to requests; and
- apply additional safeguards where appropriate.

Where information is shared about a learner, staff must consider whether the sharing is necessary, proportionate and in the learner's best interests.

---

10. PRIVACY INFORMATION

SNAP will provide appropriate privacy information explaining:

- what personal information is collected;
- why it is collected;
- the lawful basis for processing;
- who information may be shared with;
- how long information is retained;
- individuals' data protection rights;
- how concerns can be raised; and
- how to contact SNAP regarding data protection.

Privacy information provided to learners will be accessible and appropriate to their age and understanding.

---

11. INFORMATION SHARING FOR SAFEGUARDING

Data protection is not a barrier to safeguarding.

SNAP will share information when this is necessary and lawful to safeguard a learner or another person.

Staff must not refuse or delay necessary safeguarding information sharing simply because they are concerned about GDPR.

KCSIE 2026 states that data protection laws do not prevent information sharing for keeping children safe and that concerns about sharing information must not stand in the way of safeguarding and promoting children's welfare.

SNAP staff should:

- act promptly where information may be important to a safeguarding concern;
- identify the purpose for sharing;
- identify an appropriate lawful basis;
- consider whether special category data is involved;
- share information with the appropriate person or organisation;
- share information that is relevant and necessary;
- ensure information is presented clearly and in context;
- avoid unnecessary information sharing; and
- record significant information-sharing decisions and the reasons for them.

KCSIE 2026 expects information sharing to be relevant to the current safeguarding risk, necessary for the receiving setting to know, clearly presented and appropriately contextualised. Professional

judgement should be used to ensure information is focused and proportionate, while avoiding the omission of information that may be relevant to understanding or managing safeguarding risk.

---

12. SAFEGUARDING INFORMATION SHARING WITH COMMISSIONERS

As an Alternative Provision setting, SNAP will maintain appropriate arrangements with commissioning schools, academies and/or local authorities for the lawful sharing of information.

This may include information relating to:

- safeguarding;
- child protection;
- attendance;
- SEND;
- health and medical needs;
- behaviour;
- welfare;
- educational progress;
- risk assessments;
- incidents;
- exploitation;
- serious violence;
- harmful behaviours; and
- transition arrangements.

Information will be shared where there is a lawful and appropriate reason to do so.

SNAP will ensure that data protection requirements do not prevent timely safeguarding communication with the commissioning organisation.

---

13. CONFIDENTIALITY AND SAFEGUARDING

Staff must maintain an appropriate level of confidentiality.

However, confidentiality must not prevent necessary safeguarding action.

A learner must **not** be promised that information disclosed about abuse, neglect, exploitation or another safeguarding concern will remain secret.

Staff should only share information with those who need to know, such as the Designated Safeguarding Lead (DSL), deputy DSL, commissioning organisation, children's social care, police or another appropriate professional.

KCSIE 2026 requires staff to understand appropriate confidentiality and makes clear that staff should not promise a child that they will not tell anyone about a safeguarding report.

---

14. RECORDING INFORMATION-SHARING DECISIONS

Where information is shared because of a safeguarding concern, SNAP will make an appropriate record.

Records should include, where applicable:

- a clear summary of the concern;
- the information shared;
- who it was shared with;
- why it was necessary;
- the lawful basis considered;
- actions taken;
- decisions made;
- the rationale for decisions;
- any advice received; and
- the outcome.

KCSIE 2026 requires safeguarding records to clearly document concerns, actions, decisions, reasons and outcomes.

---

15. CHILD PROTECTION RECORDS

Safeguarding and child protection information must be:

- accurate;
- factual;
- clear;
- securely stored;
- kept confidential; and
- accessible only to those who need to see it.

Where appropriate, safeguarding concerns should be maintained in a separate child protection record.

Records should distinguish between:

- observed facts or concerns;
- professional opinion;
- information provided by another person; and

- historic information.

KCSIE 2026 states that safeguarding records should be clear and factual and distinguish between observed concerns, professional opinion and historic information.

---

16. TRANSFER OF SAFEGUARDING INFORMATION

Where a learner moves between educational settings, SNAP will ensure that relevant safeguarding information is transferred securely and promptly in accordance with the applicable arrangements.

Where SNAP holds the learner's child protection information, the DSL will ensure that appropriate arrangements are made for its secure transfer to the receiving setting.

Information should be transferred securely and confirmation of receipt obtained where appropriate.

KCSIE 2026 states that child protection files should be transferred as soon as possible and, for in-year transfers, within 5 days, with secure transit and confirmation of receipt.

As an Alternative Provision setting, SNAP will work with the commissioning organisation to ensure safeguarding information is transferred appropriately when a placement begins, changes or ends.

---

17. INFORMATION RELEVANT TO RISK

Where information held by SNAP indicates a safeguarding risk to the learner or another person, relevant information may need to be shared with the receiving or commissioning organisation.

This may include information relating to:

- previous or current safeguarding concerns;
- serious violence;
- weapons;
- exploitation;
- harmful behaviours;
- significant behavioural risks;
- radicalisation concerns;
- relevant health or SEND needs; or
- other information necessary to keep the learner or others safe.

Information should be shared in a way that provides sufficient context and does not unfairly disadvantage the learner.

---

18. DATA SHARING WITH OTHER AGENCIES

SNAP may share information where there is a lawful basis and where sharing is necessary and proportionate.

This may include sharing information with:

- commissioning schools and academies;
- local authorities;
- children's social care;
- safeguarding partners;
- police;
- health professionals;
- SEND professionals;
- parents/carers, where appropriate;
- education and training providers;
- emergency services; and
- other relevant organisations.

Safeguarding concerns must be shared in accordance with SNAP's Safeguarding and Child Protection Policy.

---

19. RETENTION OF DATA

SNAP will not keep personal information for longer than is necessary.

Retention periods will take account of:

- legal requirements;
- safeguarding requirements;
- educational requirements;
- contractual arrangements;
- financial and employment requirements;
- commissioning arrangements; and
- operational needs.

SNAP will maintain an appropriate retention schedule.

When information is no longer required, it will be securely deleted, destroyed or disposed of.

Safeguarding records will be retained in accordance with applicable legal, safeguarding and commissioning requirements.

---

20. STAFF RESPONSIBILITIES

All staff, volunteers, contractors and other individuals working for SNAP are responsible for protecting personal information.

Staff must:

- only access information they need for their role;
- keep personal information secure;
- follow SNAP's data protection procedures;
- maintain confidentiality;
- ensure information they provide to SNAP is accurate;
- notify SNAP of changes to their personal information;
- report suspected data breaches immediately;
- use secure systems when handling personal information;
- not share passwords;
- not leave confidential information unattended;
- not discuss confidential information where it can be overheard; and
- share safeguarding information promptly where necessary.

Unauthorised disclosure, deliberate misuse or reckless handling of personal information may result in disciplinary action and, where appropriate, legal or regulatory action.

---

21. INFORMATION SECURITY

SNAP will implement appropriate technical and organisational measures to protect personal information.

This may include:

- strong passwords/passphrases;
- multi-factor authentication where available;
- appropriate access controls;
- antivirus and malware protection;
- firewalls;
- security updates and patches;
- encryption where appropriate;
- secure backups;
- secure cloud systems;
- restricted access to sensitive records;
- secure disposal of equipment;
- secure disposal of confidential paper records; and
- staff training.

Access will be provided on a **need-to-know** basis.

---

22. EMAIL AND ELECTRONIC COMMUNICATION

Staff must take particular care when sending personal or sensitive information electronically.

Staff must:

- check the recipient before sending;
- check auto-complete suggestions carefully;
- use secure systems where available;
- use appropriate encryption or password protection where required;
- avoid sending unnecessary personal information;
- use BCC where appropriate for group communications;
- not forward confidential information to personal accounts unless authorised;
- report emails sent to the wrong recipient immediately; and
- follow SNAP's Cyber Security and IT procedures.

---

23. REMOTE WORKING AND PERSONAL DEVICES

Staff must not store SNAP personal information on personal devices unless expressly authorised and appropriate security controls are in place.

Where remote access is permitted:

- approved systems must be used;
- devices must be protected by appropriate passwords/security;
- information must not be viewed in public places where confidentiality may be compromised;
- confidential paperwork must be securely stored; and
- information must not be downloaded unnecessarily.

---

24. PHYSICAL SECURITY

SNAP will take reasonable steps to protect paper records and physical equipment containing personal information.

Staff must:

- keep confidential files secure;
- lock offices and storage areas where appropriate;
- use secure filing systems;
- clear desks of confidential information when appropriate;

- securely dispose of confidential paperwork; and
- report lost or stolen equipment immediately.

---

25. PERSONAL DATA BREACHES

A personal data breach includes the loss, destruction, alteration, unauthorised disclosure of, or unauthorised access to personal information.

Examples include:

- sending information to the wrong person;
- losing a laptop or phone containing personal information;
- losing paper records;
- accidentally publishing personal information;
- unauthorised access to a computer system;
- using the wrong email address; or
- disclosing information to an unauthorised person.

All suspected breaches must be reported to the SNAP Data Protection Lead/DPO **immediately**.

SNAP will:

1. contain the breach where possible;
2. assess the risk;
3. record the incident;
4. determine whether the ICO must be notified;
5. notify affected individuals where legally required;
6. take steps to reduce harm; and
7. review the incident and implement lessons learned.

Where a breach is reportable, the ICO must generally be notified within the applicable statutory timeframe.

---

26. INDIVIDUAL DATA PROTECTION RIGHTS

Individuals have rights in relation to their personal information, subject to the relevant legal conditions and exemptions.

These may include rights relating to:

- being informed;
- access to personal information;
- rectification;
- erasure;
- restriction of processing;

- data portability;
- objection; and
- rights relating to automated decision-making, where applicable.

SNAP will respond to rights requests in accordance with current legal requirements.

---

27. SUBJECT ACCESS REQUESTS

An individual may request access to personal information SNAP holds about them.

A Subject Access Request (SAR) should be passed promptly to the Data Protection Lead/DPO.

SNAP will:

- verify identity where necessary;
- establish the scope of the request;
- search relevant systems and records;
- consider applicable exemptions;
- protect the personal information of other individuals; and
- respond within the applicable legal timescale.

Where a safeguarding concern exists, staff must consult the DSL/Data Protection Lead before releasing information.

Where the applicable **serious harm test** is met, information may need to be withheld in accordance with data protection law. KCSIE 2026 specifically highlights the importance of considering this protection in safeguarding circumstances.

Where there is uncertainty, appropriate specialist advice should be sought.

---

28. ACCURACY AND CORRECTION

Staff and learners should notify SNAP if they believe information held about them is inaccurate or incomplete.

SNAP will take reasonable steps to correct inaccurate information.

Staff must ensure that information they create or enter into SNAP systems is accurate, factual and appropriately recorded.

Safeguarding records must clearly distinguish between fact, professional opinion and historical information.

---

29. SAFEGUARDING AND INFORMATION SHARING

Where there is a safeguarding concern, SNAP staff must follow the Safeguarding and Child Protection Policy.

Data protection law should be used to support **lawful, necessary and proportionate information sharing**, rather than as a reason to prevent appropriate safeguarding action.

Staff should seek advice from the DSL, Data Protection Lead/DPO or appropriate manager where they are unsure.

However, uncertainty about data protection must not unnecessarily delay action where a learner may be at risk of harm.

KCSIE 2026 makes clear that data protection laws do not prevent safeguarding information sharing.

---

30. RECORD OF PROCESSING ACTIVITIES

SNAP will maintain appropriate records of significant processing activities where required.

These records will identify, where appropriate:

- what information is processed;
- whose information is processed;
- the purpose of processing;
- lawful basis;
- recipients;
- retention periods;
- security measures;
- international transfers; and
- controller/processor arrangements.

---

31. INTERNATIONAL TRANSFERS

SNAP will not transfer personal information outside the UK unless the transfer is permitted under applicable UK data protection law and appropriate safeguards or another lawful mechanism are in place.

---

32. THIRD-PARTY SUPPLIERS

Where SNAP uses external organisations to process personal information, it will assess their data protection arrangements and establish appropriate contractual safeguards.

This may include providers of:

- IT systems;
- cloud storage;
- learner management systems;
- payroll;
- HR systems;
- online learning platforms;
- safeguarding systems;
- CCTV;
- transport-related systems; and
- other services involving personal information.

Where required, a written data processing agreement will be in place.

---

33. STAFF TRAINING

SNAP will provide appropriate data protection training to staff.

Training will cover, where relevant:

- confidentiality;
- UK GDPR principles;
- safeguarding and information sharing;
- children's information;
- cyber security;
- phishing and email security;
- data breaches;
- secure handling of information;
- subject access requests; and
- reporting concerns.

Staff safeguarding training will also reinforce that information sharing is an important safeguarding responsibility.

---

34. DATA PROTECTION AND ALTERNATIVE PROVISION

Because SNAP provides Alternative Provision, effective information sharing between SNAP and commissioning organisations is essential.

SNAP will maintain appropriate arrangements for the timely and lawful exchange of:

- safeguarding information;
- SEND information;
- attendance information;
- behaviour information;
- welfare information;
- educational progress;
- risk information; and
- relevant transition information.

SNAP will work with commissioning schools, academies and local authorities to ensure that information necessary to safeguard and support learners is available to those who need it.

Information sharing will be:

- lawful;
- necessary;
- relevant;
- proportionate;
- secure;
- appropriately recorded; and
- focused on the learner's welfare and educational needs.

KCSIE 2026 emphasises the importance of early information sharing, clear arrangements between organisations and proportionate sharing of relevant information.

---

35. COMPLIANCE

All SNAP staff, volunteers and contractors must comply with this policy.

A deliberate or reckless breach may result in:

- investigation;
- disciplinary action;
- removal of access to systems;
- termination of contractual arrangements; and/or
- referral to the appropriate authority where necessary.

Serious breaches may also result in regulatory or legal action.

---

36. COMPLAINTS AND CONCERNS

Anyone who believes that their personal information has not been handled appropriately should raise the concern with SNAP's Data Protection Lead/DPO in the first instance.

SNAP will investigate complaints and provide an appropriate response.

Where an individual remains dissatisfied, they may contact the Information Commissioner's Office.

---

37. POLICY REVIEW

This policy will be reviewed annually or sooner where there are significant changes to:

- data protection legislation;
- ICO guidance;
- safeguarding requirements;
- Alternative Provision arrangements;
- SNAP's systems or technology; or
- the way SNAP processes personal information.

---

38. KEY REFERENCE DOCUMENTS

This policy should be read alongside the latest applicable versions of:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Keeping Children Safe in Education 2026
- Working Together to Safeguard Children 2026
- Information Commissioner's Office guidance
- SNAP Safeguarding and Child Protection Policy
- SNAP Cyber Security/IT Policy
- SNAP Records Retention Schedule
- SNAP Privacy Notices
- SNAP Information Sharing Procedures
- SNAP Data Breach Procedure
- SNAP Alternative Provision arrangements

KCSIE 2026: The September 2026 version is the current statutory guidance in force from 1 September 2026.

ICO information-sharing guidance: SNAP will have regard to current ICO guidance concerning lawful and proportionate sharing of information to safeguard children.