DATA PROTECTION POLICY

ORGANISATION	SKAPE North East Ltd	POLICY REFERENCE	P14 GDPR
UPDATED	12 November 2026	NEXT SCHEDULED REVIEW	12 November 2027
POLICY OWNER	Centre Manager / Data Protection Lead	RELATED POLICIES	Confidentiality; Safeguarding; Online Safety; Complaints

01 INTRODUCTION

SKAPE aims to ensure that personal data relating to students, parents/carers, staff, visitors and other individuals is collected, used, stored, shared and disposed of lawfully, fairly and securely.

02 SCOPE OF POLICY

This policy applies to personal data in paper and electronic form and should be read alongside SKAPE privacy notices, safeguarding procedures, records-retention arrangements and relevant information-sharing agreements.

03 LEGISLATION AND GUIDANCE

This policy reflects the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), as amended by the Data (Use and Access) Act 2025, and current guidance from the Information Commissioner's Office (ICO).

Where relevant, SKAPE will also have regard to other legislation and guidance governing particular information, including safeguarding, employment, CCTV and electronic communications. SKAPE will have regard to relevant Department for Education guidance, statutory requirements applicable to the provision, the DfE Non-school Alternative Provision Voluntary National Standards, and the requirements and procedures of commissioning schools and Local Authorities. Where a legal requirement applies specifically to a particular type of education setting, SKAPE will apply the legal framework relevant to its role while maintaining appropriate education-sector standards and protocols.

04 DEFINITIONS

TERM	MEANING
Personal data	Information relating to an identified or identifiable living individual. This may include names, identifiers, contact details, online identifiers and information about a person's physical, social or economic identity.
Special category data	Personal data requiring additional protection, including data about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric identification data, health, sex life or sexual orientation.
Processing	Anything done with personal data, including collecting, recording, organising, storing, using, sharing, altering, retrieving, erasing or destroying it.
Data subject	The identified or identifiable living individual to whom personal data relates.
Data controller	The person or organisation that determines why and how personal data is processed.
Data processor	A person or organisation processing personal data on behalf of a controller.

TERM	MEANING
Personal data breach	A security breach leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

05 THE DATA CONTROLLER

SKAPE North East Ltd is the data controller for personal data where it determines the purposes and means of processing. In some placement or commissioning arrangements, another organisation may be a separate or joint controller for particular information. Responsibilities will be considered according to the actual processing arrangement.

06 ROLES AND RESPONSIBILITIES

6.1 Centre Manager

The Centre Manager has overall responsibility for ensuring that SKAPE complies with relevant data protection obligations and for ensuring staff follow agreed procedures.

6.2 Data protection lead

SKAPE's data protection contact is the Centre Manager, who oversees implementation of this policy, supports staff with data protection matters and acts as a point of contact for individuals and the ICO where appropriate. Contact: centremanager@skape-centre.co.uk.

SKAPE will keep under review whether the organisation is legally required to appoint a formal Data Protection Officer. Where a formal DPO is required, the role will be carried out in accordance with UK GDPR requirements.

6.3 All staff

All staff and people working on SKAPE's behalf must handle personal data in accordance with this policy and must seek advice promptly if they are unsure. Staff must immediately report suspected data breaches, loss of information, inappropriate disclosure, or other data-protection concerns to the data protection lead.

07 DATA PROTECTION PRINCIPLES

SKAPE will ensure that personal data is:

- processed lawfully, fairly and transparently
- collected for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than necessary
- processed securely, with appropriate protection against unauthorised or unlawful processing and accidental loss, destruction or damage

SKAPE is also responsible for being able to demonstrate compliance with these principles.

08 COLLECTING PERSONAL DATA

8.1 Lawfulness, fairness and transparency

Before processing personal data, SKAPE will identify an appropriate lawful basis under UK GDPR. Depending on the circumstances this may include contract, legal obligation, vital interests, legitimate interests, consent, or public task where that lawful basis genuinely applies to the particular processing.

SKAPE will not describe itself as a public authority simply because it provides education or receives publicly funded placements. The appropriate lawful basis will be considered for each processing activity.

Where special category data is processed, SKAPE will also identify an appropriate condition under Article 9 UK GDPR and, where required, the DPA 2018.

Criminal-offence information, including DBS information and records of criminal allegations or convictions, requires separate safeguards. Before using it, SKAPE will identify a lawful basis and either the relevant official authority or a condition permitted by the Data Protection Act 2018. This reflects Article 10 of UK GDPR. Where the condition used for special category or criminal-offence information requires an appropriate policy document, SKAPE will have this in place, setting out safeguards and retention arrangements. Access will be limited to people who need the information for their role.

Where consent is relied upon, it must be freely given, specific, informed and capable of being withdrawn. Consent will not be used where another lawful basis is more appropriate.

8.2 Privacy information, minimisation and accuracy

Individuals will be given appropriate privacy information explaining how their personal data is used. Staff must only collect and use information that is necessary for their role and must take reasonable steps to keep information accurate and up to date.

09 SHARING PERSONAL DATA

SKAPE will share personal data where there is a lawful basis and the sharing is necessary and proportionate. This may include sharing with commissioning schools or Local Authorities, safeguarding partners, health or emergency services, examination or awarding bodies, professional advisers, regulators, law enforcement bodies, suppliers and contractors.

Consent is not always required before information can be shared. Data protection law does not prevent appropriate safeguarding information sharing. Staff must report safeguarding concerns promptly to the DSL or deputy DSL and follow SKAPE's Safeguarding Policy alongside the commissioner's relevant safeguarding procedures. The DSL will liaise with the commissioning school's DSL or local authority safeguarding contact where appropriate and safe. Information shared must be necessary and proportionate. Urgent protective action or referrals must not wait for consent, a complaint investigation or the commissioner's response. Where a concern involves the DSL, use the alternative safeguarding reporting arrangements.

Where a student is placed at SKAPE by a commissioning school or Local Authority, SKAPE may need to exchange relevant information with the commissioner for education, attendance, safeguarding, placement review and other legitimate placement purposes. Only information that is necessary and appropriate will be shared.

Where processors are used, SKAPE will carry out appropriate due diligence and ensure suitable contractual data-protection terms are in place.

International transfers of personal data will only take place where permitted by UK data protection law and appropriate safeguards are in place.

10 SUBJECT ACCESS REQUESTS AND OTHER RIGHTS

10.1 Subject access requests (SARs)

Individuals have the right to ask whether SKAPE processes their personal data and, where applicable, to receive a copy together with the information required by data protection law. A request does not have to use the words "subject access request" or be made on a particular form.

Staff who receive a request that may be a SAR must forward it promptly to the data protection lead. SKAPE may ask for information reasonably needed to confirm identity or clarify what information is being requested.

SKAPE will respond without undue delay and normally within one calendar month of receiving the request. Where information is reasonably needed to confirm identity or a representative's authority, the response period begins when that information is received. Staff must not ask for unnecessary identification or use clarification to delay a response.

Where clarification of the information requested is reasonably required to respond effectively, SKAPE may pause the response clock while awaiting that clarification. The clock pauses rather than restarts. SKAPE will explain what clarification is needed and why. A person cannot be required to narrow their request; if they confirm their original request, SKAPE will carry out reasonable and proportionate searches.

For a complex request, or a number of requests from the same person, SKAPE may extend the deadline by up to a further two months where necessary. The requester must be told about the extension and the reasons within one month of receiving the request, taking account of any lawful pause or later start date. The data protection lead will record the applicable deadline and any permitted change to it.

Information will normally be provided free of charge. A reasonable fee may be charged, or a request refused, where permitted by law, for example where a request is manifestly unfounded or excessive. Any refusal will be explained and will include information about the right to complain to the ICO.

10.2 Children and subject access requests

Personal data relating to a child is the child's personal data. A parent or carer does not automatically have a right to obtain it through a SAR simply because they have parental responsibility.

Where a request is made by or on behalf of a child, SKAPE will consider the child's competence and understanding, the nature of the information, the child's wishes where appropriate, any authority held by the person making the request, and the child's best interests. No fixed age will be treated as determinative.

10.3 Other data protection rights

Depending on the circumstances and the lawful basis being used, individuals may have rights to:

- receive privacy information about how their data is used
- ask for inaccurate personal data to be corrected
- request erasure or restriction of processing in certain circumstances
- object to processing in certain circumstances
- withdraw consent where consent is the lawful basis
- data portability in certain circumstances
- receive safeguards around solely automated decisions with legal or similarly significant effects, including information, the ability to make representations, challenge the decision and obtain human intervention where the law requires these safeguards
- complain to SKAPE and to the ICO

Requests to exercise data protection rights should be passed promptly to the data protection lead.

11 REQUESTS CONCERNING EDUCATIONAL INFORMATION

SKAPE will manage requests for student information in line with data protection law and appropriate education-sector protocols, working with the commissioning school or Local Authority where relevant. Legal responsibilities will be applied according to the role of the organisation holding the information and the arrangements under which the student is placed.

Requests for personal data held by SKAPE will be considered under data protection law. Where a request relates to the wider educational record held by a commissioning school, SKAPE will explain this and will co-operate appropriately with the commissioning school or Local Authority, including providing relevant information held by SKAPE where there is a lawful basis to do so.

12 CCTV

SKAPE uses CCTV in relevant areas of its premises for safety, security and other stated legitimate purposes. Clear signage will be used and CCTV will be operated in accordance with data protection law and current ICO guidance.

Parents/carers do not have an automatic right to view or receive CCTV footage. Any request for access will be considered in accordance with UK data protection law.

Access to CCTV footage will be restricted to authorised persons and footage will be retained only for as long as necessary for the stated purpose, subject to any need to preserve footage relating to an incident or investigation.

13 PHOTOGRAPHS AND VIDEOS

SKAPE may take photographs or videos for legitimate education, record-keeping, communication or promotional purposes. The lawful basis will depend on the intended use.

Written consent will normally be obtained for identifiable images used for marketing, publicity, the website or social media. The intended use will be explained clearly and consent may be withdrawn for future use. Withdrawal cannot always undo publication or sharing that has already lawfully taken place. For children's publicity images, staff will obtain the required parent/carer consent and take account of the student's wishes and any safeguarding restrictions. For students aged 18 or over, their own consent will normally be required; staff must not assume that a parent or carer can consent for them.

Images used for safeguarding, evidence, educational records or other operational purposes may be processed under another lawful basis where appropriate. Staff must follow the Safeguarding, Online Safety and Handheld Device and Mobile Phone policies when taking, storing or sharing images.

Staff must use authorised SKAPE-owned equipment to take photographs, video or audio of students. Images must be stored and shared through approved SKAPE systems. Consent for one purpose does not automatically cover another; staff must check the agreed use and any restrictions before publishing or sharing images.

14 DATA PROTECTION BY DESIGN AND DEFAULT

SKAPE will consider data protection at the outset of new projects, systems and processing activities. Measures include data minimisation, appropriate access controls, privacy notices, secure defaults, staff training and appropriate contracts with processors.

A Data Protection Impact Assessment (DPIA) will be completed where processing is likely to result in a high risk to individuals' rights and freedoms, including where required for new technologies or particularly sensitive processing.

15 DATA SECURITY AND STORAGE

SKAPE will use appropriate technical and organisational measures to protect personal data. These will be proportionate to the sensitivity of the information, the risks involved and the systems being used.

- paper records containing confidential information will be stored securely and not left where unauthorised people can access them
- electronic systems will use appropriate access controls, strong passwords and, where available and appropriate, multi-factor authentication
- portable devices and removable media containing personal data will be encrypted or otherwise appropriately protected
- personal data may only be taken off site or accessed remotely where this is authorised and appropriate security arrangements are followed
- staff must not use personal devices or personal accounts for SKAPE personal data unless specifically authorised and suitable safeguards are in place Any authorisation must also follow the Handheld Device and Mobile Phone and Online Safety policies, including the rules for student images.
- information shared externally must use an appropriate secure method, particularly where safeguarding, health or other sensitive information is involved
- access to personal data will be limited to those who need it for their role

16 RETENTION AND DISPOSAL OF RECORDS

Personal data will be retained only for as long as necessary for the purpose for which it is held, taking account of legal, safeguarding, contractual, insurance and operational requirements. SKAPE will maintain or follow an appropriate records-retention schedule rather than deleting information simply because it is no longer in active use.

When records reach the end of their retention period, they will be securely destroyed or anonymised unless there is a lawful reason to retain them. Paper records will be securely shredded or disposed of through an approved confidential-waste service and electronic information will be securely deleted.

17 PERSONAL DATA BREACHES

All actual or suspected personal data breaches must be reported immediately to the data protection lead. SKAPE will contain the incident, assess the risk, document the decision and take appropriate remedial action.

SKAPE will notify the ICO of a personal data breach unless it is unlikely to result in a risk to individuals' rights and freedoms. Notification must be made without undue delay and, where feasible, within 72 hours of SKAPE becoming aware of the breach. Any delay must be explained. Where a breach is likely to result in a high risk to affected individuals, they will also be informed without undue delay unless an exemption applies.

The detailed breach procedure is set out in Appendix 1.

18 DATA PROTECTION COMPLAINTS

An individual who considers that SKAPE has infringed data protection law in relation to their personal data may make a data protection complaint directly to SKAPE.

SKAPE will facilitate complaints, including by accepting complaints electronically through admin@skape-centre.co.uk or by other reasonable means. A complaint will be acknowledged within 30 days. SKAPE will take appropriate steps to investigate the complaint without undue delay, keep the complainant informed of progress where appropriate, and notify them of the outcome.

The complainant will be told that they may raise their concern with the Information Commissioner's Office if they remain dissatisfied. Data protection complaints may also be considered alongside P13 Complaints Policy where appropriate, but the statutory data-protection complaint process will not be restricted by the general complaints procedure.

If the complaint concerns the data protection lead or Centre Manager, it should be addressed privately to an uninvolved Director using the contact arrangements in the Complaints Policy. If no uninvolved Director is available, SKAPE will use the impartial handling arrangements in that policy. This must not require the complainant to complete the general complaints stages or delay the separate data-protection complaint process or any legal deadline.

19 TRAINING

All staff will receive appropriate data-protection training as part of induction and refresher training where necessary. Additional guidance or training will be provided where legislation, ICO guidance, systems or SKAPE processes change.

20 MONITORING ARRANGEMENTS

The Centre Manager, as data protection lead, will monitor this policy and make sure significant issues are brought to any other relevant responsible person. The policy will be reviewed annually, or sooner where there is a significant change in law, guidance, technology or SKAPE practice.

21 LINKS WITH OTHER POLICIES

- Safeguarding Policy
- Online Safety Policy
- Confidentiality Policy
- Complaints Policy
- Staff Acceptable Use / ICT arrangements
- Records-retention and privacy information where applicable
- Handheld Device and Mobile Phone Policy
- Employee Code of Conduct
- Whistleblowing Policy

22 DOCUMENT REVISION HISTORY

DATE	CHANGE	APPROVAL	REV.
10/07/2023	Initial policy	K. Watson	01
01/03/2025	Policy review	K. Watson	02
01/09/2025	Policy review	K. Watson	03
20/09/2026	Policy review — updated for current data protection law and SKAPE status	K. Watson	04
12/11/2026	SKAPE branding and layout standardised; roles and terminology updated; subject-access deadlines, breach reporting, sensitive information, images, safeguarding liaison and impartial complaint handling aligned with current guidance and related policies.	L. James	05

23 APPENDIX 1 PERSONAL DATA BREACH PROCEDURE

This procedure is based on current ICO guidance. Any staff member or processor who discovers or suspects a personal data breach must immediately notify the data protection lead.

- The data protection lead will establish what happened, what personal data is affected, whose data is involved, and whether the breach is continuing.
- Immediate steps will be taken to contain the breach and reduce harm. This may include recalling an email, restricting access, recovering a device, changing credentials, contacting an unintended recipient or obtaining specialist IT support arranged by the Centre Manager.
- The Centre Manager will oversee significant breaches and ensure that other relevant responsible roles are informed where necessary.
- The likely consequences and risk to individuals' rights and freedoms will be assessed, taking account of the sensitivity and volume of data, the people affected, the circumstances of disclosure and the likelihood and severity of harm.
- The ICO must be notified unless the breach is unlikely to result in a risk to individuals' rights and freedoms. The decision and reasons must be recorded. Where notification is required, it must be made without undue delay and, where feasible, within 72 hours of SKAPE becoming aware of the breach. Any delay must be explained.
- If all information is not available within 72 hours, SKAPE may provide information in phases and explain any delay.
- Where the breach is likely to result in a high risk to affected individuals, they will be informed without undue delay unless an exemption applies.
- All personal data breaches will be recorded, including the facts, effects, assessment, decisions and remedial action, whether or not they are reported to the ICO.
- After a significant breach, the data protection lead will review the incident with relevant staff and identify any changes needed to systems, procedures, training or controls.

Actions to minimise the impact of common breaches

Examples of immediate action include:

- Email sent to the wrong recipient: attempt recall where available; contact the recipient promptly; ask them to delete the information and not share or retain it; consider whether further containment or notification is required.
- Lost or stolen device: report immediately; establish whether the device was encrypted and remotely manageable; change relevant credentials; contact the Centre Manager to arrange specialist IT support and, where appropriate, the police; assess the data-protection risk.
- Unauthorised access to safeguarding or special category information: restrict access immediately, preserve relevant evidence, inform the DSL where safeguarding information is involved, and assess whether the commissioner or another agency needs to be informed.
- Information published online in error: remove or restrict access as quickly as possible, consider cached or copied versions, contact the platform or website administrator where necessary, and assess notification requirements.

Staff must not decide for themselves that a breach is "too minor" to report internally. Prompt internal reporting allows SKAPE to assess risk and meet any statutory time limits.