



Auckland College Independent School

Every Pupil Matters, Every Moment Counts

Data Protection Policy





Document Control

Owner:	Auckland College Independent School
Written by:	Mrs Stephanie Livramento & Mr Lorenzo Willis
Approved by:	Mr Anthony Akaraonye – Chair of Governors
Applies to:	Whole School
Date effective from:	9 September 2026
Review period:	1 Year
Date of next review:	9 September 2027
Version:	V1



Purpose and scope

Auckland College Independent School is committed to protecting personal data and respecting the privacy rights of pupils, parents and carers, staff, applicants, volunteers, contractors, visitors and other individuals whose information it processes. This policy explains the principles and arrangements the school uses to ensure personal data is handled lawfully, fairly, transparently and securely.

This policy applies to personal data in any format, including information held electronically, on paper, in photographs, audio or video recordings, CCTV systems, email, cloud services and school information systems. It applies to all staff and others who process personal data on behalf of the school.

Legal and regulatory framework

The school will process personal data in accordance with applicable UK data protection law, including:

- the UK General Data Protection Regulation (UK GDPR);
- the Data Protection Act 2018 (DPA 2018), as amended;
- the Data (Use and Access) Act 2025 (DUAA), including amendments to the UK GDPR and DPA 2018 that are in force;
- the Privacy and Electronic Communications Regulations 2003 (PECR), where relevant; and
- relevant guidance and statutory codes issued by the Information Commissioner's Office (ICO).

The DUAA does not replace the UK GDPR or DPA 2018. It amends aspects of the existing framework, including provisions concerning subject access, recognised legitimate interests, automated decision-making, international transfers and data protection complaints.

Definitions

- **Personal data:** information relating to an identified or identifiable living individual.
- **Special category data:** particularly sensitive personal data, including information concerning health, racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, genetic or biometric data used for identification, and data concerning sex life or sexual orientation.
- **Processing:** any operation performed on personal data, including collecting, recording, organising, storing, altering, retrieving, using, sharing, restricting or deleting it.
- **Data subject:** the individual to whom personal data relates.
- **Controller:** the organisation that determines why and how personal data is processed. Auckland College is the controller for the personal data it determines the purposes and means of processing.
- **Processor:** a person or organisation processing personal data on the controller's behalf.



- Personal data breach: a security breach leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Data protection principles

The school is responsible for, and must be able to demonstrate, compliance with the data protection principles. Personal data will be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes and not used incompatibly with those purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- kept in identifiable form for no longer than necessary;
- processed with appropriate security, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage; and
- managed in a way that demonstrates accountability.

Roles and responsibilities

5.1 Proprietors and senior leadership

The Proprietors and senior leadership are responsible for ensuring that appropriate governance, resources and oversight are in place for data protection compliance.

5.2 Headteacher / Data Protection Lead

The Headteacher has overall operational responsibility for implementation of this policy and for ensuring that concerns, rights requests, breaches and data protection complaints are handled appropriately. The school will appoint a Data Protection Officer where the legal criteria require one. Where no statutory DPO is required, the school will maintain a clearly identified Data Protection Lead and obtain specialist advice when necessary.

5.3 All staff

All staff must protect personal data, follow school procedures, complete required training, use only authorised systems, report suspected breaches immediately and seek advice before undertaking unfamiliar or high-risk processing.

Lawful processing

Before processing personal data, the school will identify and document an appropriate lawful basis under Article 6 UK GDPR. Depending on the circumstances, this may include legal obligation, contract, vital interests, legitimate interests, recognised legitimate interests introduced through the DUAA, consent, or another applicable lawful basis.

The school will not rely on consent where another lawful basis is more appropriate. Where consent is relied upon, it must be freely given, specific, informed and unambiguous, and capable of being withdrawn.

Where special category data is processed, the school will also identify an applicable condition under Article 9 UK GDPR and, where required, Schedule 1 of the DPA 2018.



Criminal offence data will be processed only where the law permits and appropriate safeguards are in place.

Children's personal data

Children merit particular protection in relation to their personal data. The school will explain its use of personal data in clear, age-appropriate language where information is provided directly to pupils, and will take account of a child's competence, best interests and rights when responding to requests concerning their information.

Safeguarding information may be processed or shared without consent where there is an appropriate lawful basis and doing so is necessary and proportionate to protect a child or another person. Data protection law does not prevent appropriate safeguarding information sharing.

Privacy information and transparency

The school will provide appropriate privacy information explaining, in clear language, what information it collects, why it uses it, the lawful basis relied upon, who it may be shared with, how long it is retained, relevant rights and how to raise a concern.

Separate or tailored privacy notices may be used for pupils and parents/carers, staff, job applicants, visitors, CCTV and other categories where appropriate. Privacy information will be reviewed when processing activities or legal requirements change.

Individual rights

Individuals have rights under data protection law, subject to applicable conditions and exemptions. These include rights to be informed, to access personal data, to have inaccurate data rectified, and in certain circumstances to erasure, restriction, objection and data portability. Individuals may also have rights relating to automated decision-making.

The school will facilitate the exercise of these rights and will not normally charge a fee. A reasonable fee may be charged, or a request refused, only where the law permits.

Subject access requests

A subject access request (SAR) is a request by an individual for access to their personal data. Requests do not need to use particular wording or a school form and may be made verbally or in writing.

The school will respond without undue delay and normally within one month, subject to lawful extensions or pauses. In accordance with the framework as amended by the DUAA, the school may seek information reasonably required to identify the information or processing activities to which a request relates, and the applicable response period may be paused while awaiting necessary clarification. Searches will be reasonable and proportionate.

The identity of the requester and their entitlement to receive the information will be verified where reasonably necessary. Information about other people will be protected



and exemptions will be applied where appropriate. Requests concerning a child's data will be considered in light of the child's competence, rights and the circumstances of the request.

Accuracy, retention and disposal

Reasonable steps will be taken to ensure personal data is accurate and kept up to date. Individuals should inform the school when relevant information changes.

Personal data will be retained only for as long as necessary for the purpose for which it is held, taking account of legal, safeguarding, educational, employment, insurance and regulatory requirements. Detailed retention periods will be set out in the school's records retention schedule.

When information is no longer required, it will be securely deleted, destroyed or anonymised as appropriate. Paper records containing confidential information will be disposed of securely.

Data sharing

Personal data will be shared only where there is a lawful basis and the sharing is necessary, proportionate and appropriately secure. The school may share information with, for example, parents/carers where appropriate, other schools, examination bodies, local authorities, government departments, safeguarding partners, health professionals, emergency services, professional advisers, insurers and service providers.

Where safeguarding or the prevention or detection of crime is involved, information may be shared without consent where the law permits. Staff must not allow concerns about data protection to prevent necessary and proportionate safeguarding action.

Where another organisation processes data on the school's behalf, the school will use appropriate contractual arrangements and carry out proportionate due diligence.

Information security

The school will use appropriate technical and organisational measures to protect personal data. Measures will be proportionate to the nature and risk of the processing and may include:

- role-based access controls and the principle of least privilege;
- strong passwords and multi-factor authentication where available and appropriate;
- approved school devices, systems, cloud services and communication channels;
- secure configuration, updates, malware protection, filtering and monitoring controls where relevant;
- secure storage and transfer of confidential records;
- regular backups and appropriate recovery arrangements;
- physical security for paper records and devices;
- secure disposal of records and equipment; and



- staff training and procedures for recognising phishing, misdirected communications and other security risks.

Personal data must not be stored or transferred using unauthorised personal accounts, applications, devices or removable media.

Personal data breaches

Any actual or suspected personal data breach must be reported immediately to the Headteacher/Data Protection Lead. Staff must preserve relevant information, follow instructions and must not attempt to conceal or independently resolve a serious breach.

The school will record and assess breaches, take steps to contain and mitigate harm, and determine whether notification is required. Where a breach is likely to result in a risk to people's rights and freedoms, the school will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it. Where a breach is likely to result in a high risk, affected individuals will also be informed without undue delay unless an applicable exception applies.

Photographs, video, audio and CCTV

Images, video and audio recordings that identify individuals are personal data. The school will identify an appropriate lawful basis for their use and will provide relevant privacy information.

CCTV will be used only for specified purposes such as safety, security and the prevention or investigation of incidents. Access to recordings will be restricted, retention will be controlled, and disclosure will be made only where lawful and appropriate.

Use of pupil images for publicity, marketing or other optional purposes will be managed in accordance with the school's privacy information and consent arrangements where consent is the appropriate lawful basis.

Online systems, AI and automated decision-making

Staff must use only school-approved digital services for processing personal data. Before introducing significant new systems, including artificial intelligence tools, the school will consider data protection, security, confidentiality, contractual terms, children's rights and whether a Data Protection Impact Assessment is required.

Personal or confidential pupil, family or staff information must not be entered into public or unapproved generative AI services.

Where the school uses solely automated processing to make a decision that produces legal or similarly significant effects, it will ensure that the processing is lawful and that applicable safeguards are provided, including appropriate information, the opportunity to make representations or challenge a decision, and human intervention where required.

Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) will be completed where processing is likely to result in a high risk to individuals' rights and freedoms. The school will also use DPIAs as good practice for significant new technologies or processing involving sensitive or large-scale information where risk warrants it.



DPIAs should consider necessity, proportionality, risks to individuals and measures to reduce those risks before the processing begins.

International transfers

Personal data will not be transferred outside the UK unless the transfer complies with the applicable UK data protection rules. The school will ensure that an appropriate transfer mechanism or other lawful basis is in place and will assess relevant protections where required.

Training and confidentiality

Staff with access to personal data will receive appropriate data protection and information security training. Training will be refreshed periodically and when significant legal, technological or procedural changes occur.

All staff and others authorised to access personal data are expected to maintain confidentiality. Deliberate, reckless or serious breaches of this policy may be dealt with under the school's disciplinary or contractual procedures.

Data protection complaints

Anyone who is concerned about how the school has handled their personal data should contact the school in the first instance. The school will maintain an accessible process for receiving and handling data protection complaints, including an electronic means of submitting a complaint where required by law. Complaints will be acknowledged, investigated appropriately and the complainant will be informed of the outcome and of any further rights.

Individuals also have the right to raise concerns with the Information Commissioner's Office (ICO). The school will cooperate with the ICO and other competent regulators as required.

Records and accountability

The school will maintain appropriate records to demonstrate compliance. Depending on the processing involved, these may include records of processing activities, lawful-basis decisions, privacy notices, data sharing arrangements, processor contracts, DPIAs, consent records, breach records, rights requests, complaints, retention decisions and staff training.

Policies, systems and processing activities will be reviewed periodically and when significant changes occur.

Related school documents

- Privacy notices
- Records Retention Schedule
- Safeguarding / Child Protection Policy
- Online Safety Policy
- CCTV Policy
- Staff Acceptable Use / IT policies



- Freedom of Information arrangements where applicable
- Records of Processing Activities
- Data breach procedure and breach log
- Subject access / individual rights procedure
- Data Protection Impact Assessment procedure

Monitoring and review

This policy will be reviewed at least annually and sooner where there is a significant change in legislation, ICO guidance, school systems or the nature of the school's processing. The Headteacher will ensure that material changes are communicated to relevant staff and that associated privacy information and procedures are updated where necessary.

Appendix 1 - Immediate staff actions

Situation	What staff should do
Email or document sent to the wrong person	Report immediately to the Headteacher/Data Protection Lead; do not rely only on recalling or deleting the message.
Device, file or paper record lost or stolen	Report immediately and provide details of the information involved and security measures in place.
Suspicious email, phishing attempt or compromised account	Stop, report through the school's IT/security route and inform the Headteacher/Data Protection Lead if personal data may be affected.
Request for a copy of personal information	Treat it as a potential rights request/SAR and forward promptly; do not insist that the requester completes a particular form.
Request from an outside organisation for pupil/staff data	Do not disclose automatically. Verify the requester, purpose and lawful basis, and seek advice if unsure.
Safeguarding concern requiring information sharing	Follow the safeguarding procedure. Share necessary and proportionate information with appropriate people; data protection should not be used as a reason to delay safeguarding action.
Considering a new app, AI tool or online service	Do not upload personal data until the service has been approved and data protection/security implications have been assessed.



Appendix 2 - Key external references

This policy has been updated with reference to the UK GDPR and Data Protection Act 2018, the Data (Use and Access) Act 2025 and current government/ICO information available at the date of review. The DUAA received Royal Assent on 19 June 2025; the majority of its data protection and privacy provisions in Part 5 were brought into force on 5 February 2026, and the ICO states that all data protection provisions were in force by 19 June 2026.

- GOV.UK - Data protection: the UK's data protection legislation
- GOV.UK - Data (Use and Access) Act 2025: data protection and privacy changes
- GOV.UK - Data Use and Access Act 2025: plans for commencement
- Information Commissioner's Office - Data Use and Access Act 2025: summary of changes