



SAFE START SCHOOL

WILLPOWER-INITIATIVE-SUCCESS-EMPATHY-RESPECT

Created by:	Grace Speakman
Reviewed Date:	October 2026
Review Due:	October 2027
Verified by:	Rachel Pilling

Purpose and scope

Safe Start School protects personal information while using and sharing it lawfully to educate pupils, support staff and safeguard welfare. This policy applies to employees, governors, directors, volunteers, agency staff and contractors who handle information for the school, on or off site. It covers electronic records, emails, paper, photographs, video, audio and personal information held in school systems or by service providers.

The data controller is Safestart School Ltd, the school's proprietor. This policy supports compliance with the UK GDPR, Data Protection Act 2018 and Privacy and Electronic Communications Regulations 2003, as amended, including relevant changes made by the Data (Use and Access) Act 2025. It also reflects Keeping children safe in education 2026. DfE school guidance is applied with regard to the school's independent status.

Read this alongside safeguarding, safer recruitment, retention, acceptable use, staff mobile phone, photography, CCTV and business continuity policies, and the school's privacy notices. Confidential business information is also subject to the security controls in this policy even where it is not personal data.

Definitions and principles

Personal data is information relating to an identifiable living person. Processing includes collecting, viewing, recording, storing, changing, sharing and deleting it. Special category data includes health, disability, ethnicity, religion and biometric data used for unique identification. Criminal offence information is subject to separate legal safeguards. Pseudonymised information remains personal data where identification is possible.

Personal data must be processed lawfully, fairly and transparently; collected for specified legitimate purposes; limited to what is needed; accurate and kept up to date; retained only as long as necessary; and protected against unauthorised use, loss, damage or destruction. The school must demonstrate compliance through records, decisions, training and proportionate checks.

Accountability and responsibilities

The proprietor remains accountable for compliance and provides resources and oversight. The Headteacher implements this policy and ensures cover for key roles. *Grace Speakman* is the school's designated Data Protection Officer (DPO) and operational contact through the school office and coordinates advice, requests, complaints, breaches and compliance records. Staff must not delay reporting because *Grace* is unavailable: contact the Headteacher or proprietor immediately.

The DPO advises on data protection, monitors compliance, advises on impact assessments and acts as a contact for individuals and the ICO. The proprietor will ensure the role is independent, suitably skilled, resourced and free of conflicting duties, with direct access to senior leadership. DPO contact details must be published in privacy information and notified to the ICO. Compliance decisions remain the controller's responsibility; IT providers manage technical controls under school oversight.

Lawful bases and sensitive information

Before processing begins, the school will record the purpose and appropriate Article 6 lawful basis. These may include legal obligation, contract where necessary for a contract with the individual, vital interests, consent, legitimate interests or public task where a specific legal function supports it. Independent school status does not automatically establish a public task basis. Consent will not be used to imply a choice where processing is compulsory.

Ordinary legitimate interests requires a documented assessment of purpose, necessity and the effect on individuals, with particular care for children. The recognised legitimate interests basis introduced by the Data (Use and Access) Act may be used only where the particular statutory condition and necessity test are met, including applicable safeguarding purposes. It is not a blanket exemption and does not remove transparency or sensitive-data requirements.

For special category information, an Article 9 condition must also be identified and, where required, a relevant Data Protection Act Schedule 1 condition. Criminal offence data requires Article 10 authority or an applicable domestic-law condition. An appropriate policy document will be maintained where required, explaining safeguards and retention. Staff must not assume parental agreement alone authorises every use of EHCP, medical, safeguarding or DBS information.

Privacy information consent and pupil rights

Pupils, families, staff and applicants will receive clear privacy information identifying the controller, contact arrangements, purposes, bases, recipients, retention criteria, rights and complaint routes. Relevant information about overseas transfers, sources of indirectly obtained information and automated decisions will also be provided. Notices must be accessible, available when information is collected or within the applicable deadline for indirect collection, and updated when processing changes.

Where consent is used, it must be a specific, informed, freely given positive choice and be recorded. It must be as easy to withdraw as to give. Silence is not consent. Optional identifiable publicity follows the Photography Policy and its separate choices. Consent is not renewed automatically each year: permissions are checked for continuing validity, with periodic reminders and fresh consent for new uses or changed circumstances. Any annual policy review of permissions does not itself require a new consent form.

Information rights belong to the pupil. Understanding and authority will be assessed for the particular decision, with communication support and reasonable adjustments. SEND does not itself mean a pupil lacks capacity. A parent does not automatically have unrestricted access to a child's information or authority to act for an adult pupil. For pupils aged 16 or over, relevant capacity decisions follow the Mental Capacity Act where applicable. The online-service consent age of 13 is not a general school-data rule.

Records and data minimisation

The school will keep a record of processing activities covering purposes, information categories, individuals, recipients, lawful bases, sensitive-data conditions, transfers, security and retention. Recurring pupil, staff and safeguarding processing must not be assumed exempt merely because the school is small. Information assets, systems, processor contracts, impact assessments and key decisions will be recorded.

Collect only necessary information and use secure forms and approved systems. Check accuracy at collection and when circumstances change. Distinguish facts from professional opinion, record sources and dates, and correct inaccuracies without obscuring the history of a safeguarding or employment decision. Access is granted by role and need, not simply

because someone works at the school.

Sharing and safeguarding

Staff may share relevant information lawfully for education, SEND support, attendance, health or safeguarding with authorised recipients, including local authorities, social care, police and health professionals. Verify identity, authority, purpose, lawful basis and the minimum necessary information. Use approved secure routes and record significant disclosures and reasons, including reasons for deciding not to share where relevant.

Data protection law does not prevent necessary, proportionate safeguarding sharing. Consent is not always required and must not be sought where doing so could increase risk or prejudice protection. Staff must consult the DSL where possible, but must not delay urgent safeguarding action while waiting for consent or a data protection sign-off. Apply KCSIE and the school's safeguarding procedures, including relevant information-sharing duties in force. Inform individuals unless a lawful safeguarding or other exemption justifies withholding that information.

EHCP consultations, pupil transfers and alternative provision arrangements require particular care. Check addresses and recipient lists, avoid unnecessary whole-file disclosures, establish responsibilities and secure exchange arrangements, and confirm safe receipt of sensitive records. Safeguarding transfers follow their specific statutory guidance and deadlines. Do not treat all information held by another organisation as automatically available to the school.

Individual rights and subject access requests

People may have rights to information, access, correction, erasure, restriction, portability and objection, depending on the lawful basis and circumstances. Erasure is not absolute; necessary safeguarding, statutory and legal-claim records may need to be retained. Staff must forward any request to *Grace Speakman* or the Headteacher immediately, recording the date received. Requests can be verbal or written and need not mention data protection or use a particular form.

Subject access requests will normally be answered without undue delay and within one calendar month. A lawful extension of up to two further months may apply because of complexity or the number of requests; the person must be informed within the initial month with reasons. Identity or representative authority checks must be necessary and proportionate and requested promptly. Calculate the deadline under current ICO rules, including any justified identity-check requirements.

Make reasonable and proportionate searches of relevant records, including school email, paper and approved cloud systems. If clarification is reasonably necessary to identify the information or processing activities requested, ask promptly and apply the statutory clock-pause rules, explaining the effect. Do not force the person to narrow their request or use clarification to delay. Preserve relevant information; do not alter or destroy it to frustrate access.

Before disclosure, assess information about other people, legal privilege and applicable education, health, social work or safeguarding exemptions case by case. Redact where appropriate and explain any withholding unless an exemption permits otherwise. Parent requests require consideration of pupil competence, authority, welfare and any separate statutory access rights; do not assume maintained-school educational-record rules automatically apply to this independent school.

Responses will be sent securely and include required supplementary privacy information. Access is normally free. Only apply a fee or refuse a manifestly unfounded or excessive request where the legal test is met and reasons are recorded. Explain applicable refusal reasons and the right to complain to the ICO and seek a judicial remedy. Large volume alone is not grounds for refusal.

Information security and staff conduct

Use approved school accounts, systems and storage. Do not send school personal data through private email, personal messaging, personal cloud storage or unapproved removable media. Contractor status does not create an exception. Personal-device access requires an expressly approved managed arrangement consistent with other policies; personal devices must never be used to capture or store pupil photographs under the Photography Policy.

Use individual accounts, least-privilege access, separate administrator accounts and multi-factor authentication for email, remote access, administrative accounts and other sensitive services where supported. Use strong unique passwords or passphrases and an approved password manager. Passwords must not be shared or displayed. Change compromised passwords promptly; routine forced changes are not a substitute for strong authentication. IT will apply proportionate minimum settings and block common passwords where possible.

Lock screens whenever leaving a device, with automatic locking after no more than ten minutes of inactivity. Keep paper records and portable devices secure; use encryption on school laptops and approved removable storage. Do not leave devices or records in vehicles unless unavoidable and authorised precautions are in place; keep them concealed and remove them promptly. Protect confidentiality when working remotely or discussing cases and collect printouts without delay.

Check recipients, attachments and sharing permissions before sending. Use secure portals, restricted links or encrypted attachments for sensitive transfers; communicate attachment passwords separately. BCC may be used for suitable non-sensitive group messages, but is not enough for high-risk bulk communication. A “confidential” label alone does not secure information. Do not automatically delete source emails: retain or dispose of them according to their record value and retention schedule.

Only authorised IT personnel may install software, approve remote-access tools or change security settings. Maintain an asset register, supported operating systems, security updates, malware protection, firewalls and appropriate logs. Prioritise critical vulnerabilities promptly; cost or a major-version change is not a reason to leave unsupported software in use without a documented mitigation and replacement decision. Scan removable media and investigate security alerts promptly.

Backups continuity and disposal

School files are stored in Google Drive. The school does not currently maintain a separate backup copy. The Headteacher, with IT support, will verify the recovery facilities available, record their limitations and assess whether additional backup arrangements are needed. Recovery procedures and responsibilities will be documented and tested periodically.

The retention schedule will specify record categories, purposes, retention periods or criteria, review triggers and secure disposal. Do not retain everything indefinitely or delete all pupil information on leaving. Suspend routine disposal where a request, complaint, investigation, safeguarding need or legal hold requires preservation. Review unnecessary copies and

securely shred paper and sanitise storage before reuse or disposal, obtaining provider assurance where appropriate.

Apply documented backup expiry and deletion arrangements; data awaiting deletion must not be returned to active use. Remove access promptly when roles change or staff leave, recover devices and records, and close or transfer accounts securely. Confidential paper and electronic material must not enter ordinary waste.

Suppliers cloud systems and overseas transfers

Before procurement, establish whether a supplier is a processor, independent controller or joint controller. Assess security, confidentiality, reliability, subcontractors, deletion, audit support, data location, transfers and incident reporting. Processor contracts must contain the Article 28 terms and require notification to the school without undue delay after awareness of a breach. Agree responsibilities for rights requests and return or secure deletion at contract end.

Personal data must not be uploaded to a new app, cloud service or online learning platform until the Headteacher and data protection lead have approved the arrangement with IT and safeguarding advice. Establish whether overseas hosting or access creates a restricted transfer. Where required, use an adequacy regulation or appropriate safeguards such as the UK International Data Transfer Agreement or UK Addendum, with the applicable data protection test and supplementary measures. Record the decision and inform individuals appropriately.

Privacy by design impact assessments and AI

Build privacy into new systems and changes: use minimum data, restricted defaults, clear notices and proportionate safeguards. Complete a Data Protection Impact Assessment before processing likely to create a high risk, including relevant monitoring, sensitive-data combinations and new technologies. Seek advice from the school's DPO. Consult the ICO before proceeding if high residual risk cannot be reduced sufficiently.

Do not put identifiable pupil, family or staff information into public or unapproved generative AI services. Proposed AI use needs prior approval and assessment of necessity, accuracy, bias, supplier access, model training, security, retention, transfers and human review. Anonymous examples must be genuinely non-identifiable. Pupil images and voices are also subject to the Photography Policy. AI output must be checked before it informs a record or decision.

The school will not introduce solely automated decisions with legal or similarly significant effects, such as admissions or employment decisions, without a specific legal assessment and approval. Any permitted use must meet applicable safeguards, transparency, representation, challenge and human-intervention requirements; special category data has additional restrictions. Meaningful human review must not be a rubber stamp.

Photography CCTV monitoring and communications

Follow the Photography Policy and current consent choices for optional images. Keep the permissions record accessible to relevant staff, restrict sensitive reasons to those who need them and check before capture and publication. Essential school uses need their own basis. Consent can be withdrawn verbally or in writing; continuing consent-based use must stop and school-controlled copies be addressed promptly.

CCTV, security audio, filtering and monitoring require defined purposes, necessity and proportionality checks, privacy information, controlled access and suitable retention. Audio is particularly intrusive and needs specific justification and safeguards; camera approval does not automatically justify sound recording. Follow the separate CCTV DPIA and policy. Pupils and staff will be informed of monitoring except where a specific lawful exception applies.

Electronic marketing and website cookies or similar technologies must be assessed under PECR as well as data protection law. Separate required school communications from promotional messages. Obtain consent where required, provide appropriate opt-out routes and respect preferences. Do not assume a general photography form authorises marketing communications or non-essential cookies.

Personal data breaches and immediate action

A breach includes accidental or unlawful loss, destruction, alteration, unauthorised disclosure or access, including unavailable records, misdirected emails, lost paper files and compromised accounts. Report actual or suspected breaches immediately to *Grace Speakman* and the Headteacher, including outside normal hours through available school emergency arrangements. If unavailable, escalate to the proprietor; do not wait two working days. Inform the DSL at once where a pupil may be at risk and involve authorised IT support for technical incidents.

Staff should take safe immediate containment steps, such as stopping an incorrect send, withdrawing a shared link or disconnecting a suspected compromised device from the network where advised, without destroying evidence or undertaking an unauthorised investigation. Do not conceal an error, contact affected people independently or delete evidence. The lead will record awareness time, affected data and people, likely consequences, containment and further actions.

Assess risk to people immediately. Notify the ICO without undue delay and, where feasible, within 72 hours of awareness unless the breach is unlikely to create a risk to rights and freedoms. The period includes weekends and holidays. If information is incomplete, make an initial report and provide updates; record reasons for any delay. Where a breach is likely to result in high risk, inform affected people without undue delay unless a lawful exception applies.

Keep a log of every personal data breach, including those not reported externally, the reasons for notification decisions, remedial action and lessons learned. The Headteacher and proprietor ensure cover so that statutory deadlines can be met. Review access, controls, training and continuity arrangements after incidents; notify other bodies where a separate duty or contractual requirement applies.

Data protection complaints

Anyone may complain about how the school handles personal information by speaking to or writing to the school office, *Grace Speakman* or the Headteacher. Staff must help people submit complaints, including electronically or with accessible support, without insisting on a special form. Forward complaints immediately, log them and preserve relevant evidence. Complaints involving the usual handler will be referred to an appropriate alternative, including the proprietor.

Acknowledge a data protection complaint within 30 days of receipt. Investigate appropriately without undue delay, make necessary enquiries, keep the person informed and communicate the outcome and action taken without undue delay. Explain the right to complain to the

Information Commissioner's Office at ico.org.uk and any available internal review. A related information-rights request or breach retains its own deadline; the complaint process does not suspend it.

Training oversight and review

Staff receive data protection and security training at induction and periodic refreshers appropriate to their roles, including recognising rights requests, secure sharing, phishing and immediate breach reporting. Leaders will check implementation through proportionate audits of access, retention, suppliers, notices, requests, complaints and incidents. Deliberate or negligent breaches may lead to action under employment or contractual procedures; reporting an honest error promptly supports effective containment.

This October 2026 revision replaces the previous policy on adoption and will be reviewed annually or earlier following relevant legal, guidance, technology or organisational changes. The school will maintain its ICO registration and fee payment where required. Key reference sources are the ICO's UK GDPR guidance, DUAA guidance, subject access and complaints guidance; DfE Data protection in schools; KCSIE 2026; and NCSC school cyber security guidance.