Data Protection & GDPR Policy
(Including CCTV)

(Independent School Standards: Parts 15 & 34)

Important note: The term 'Spark' or 'Spark Academy Group' applies to both our tutoring and independent school settings, also referred to as 'provision', 'school' or 'organisation' interchangeably.

Guidance & Legislation

- The Data Protection, Privacy & Electronic Communications
- Data Protection Act 2018
- Information Commissioners Office
- The Education (Pupil Information) (England) Regulations 2005

Last External Review	August 2025
Next External Review	August 2026
Last Update	September 2025
Author	CEO / Proprietor
Policy Sign Off	Headteacher

We Build Communities Where Everyone Belongs, Grows & Thrives.

Contents

Section 1: Introduction

Aim

Spark aims to ensure that all personal data collected about staff, pupils, parents,, visitors and other individuals is collected, stored and processed in accordance with UK data protection law. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Definitions

Personal Data

Any information relating to an identified, or identifiable, living individual. This may include the individual's:

- Name (including initials)
- Identification number
- Location data
- Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Special Categories of Personal Data

Personal data which is more sensitive and so needs more protection, including information about an individual's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics
- Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes
- Health - physical or mental
- Sex life or sexual orientation

Processing

Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data Subject

The identified or identifiable individual whose personal data is held or processed.

Data Controller

A person or organisation that determines the purposes and the means of processing of personal data.

Data Processor

A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

Personal Data Breach

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

Section 2: The Data Controller

Our school processes personal data relating to parents, pupils, staff, visitors and others, and therefore is a data controller. The school is registered with the ICO / has paid its data protection fee to the ICO, as legally required.

Section 3: Roles & Responsibilities

This policy applies to all staff employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

The Proprietor

The Proprietor has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

The Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the head of provision and, where relevant, report to the Head their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO. Full details of the DPO's responsibilities are set out in their job description. Our DPO is **Caroline Burgess from the DPO Centre** and is contactable via email/phone through the school office.

The Headteacher

The Headteacher acts as the representative of the data controller on a day-to-day basis.

All Staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this polic
- Informing the school of any changes to their personal data, such as a change of address

Contacting the DPO in the following circumstances:

- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- If they have any concerns that this policy is not being followed
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

Section 4: Data Protection Principles

The UK GDPR is based on data protection principles that our school must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure This policy sets out how the school aims to comply with these principles.

Section 5: Collecting Personal Data

Lawfulness, Fairness & Transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual or another person i.e. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task in the public interest or exercise its official authority
- The data needs to be processed for the legitimate interests of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given explicit consent
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for the establishment, exercise or defence of legal claims
- The data needs to be processed for reasons of substantial public interest as defined in legislation
- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law.

Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given consent
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- The data needs to be processed for reasons of substantial public interest as defined in legislation Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law. We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

Limitation, Minimisation & Accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up-to-date.

Inaccurate data will be rectified or erased when appropriate. In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

This will be done in accordance with the school's record retention schedule.

Section 6: Sharing Personal Data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies.
- We will also share personal data with law enforcement and government bodies where we are legally required to do so.
- We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff. If/Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law
- Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service

Section 7: Subject Access Requests & Other Rights of Individuals

Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them.

This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority

- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request in any form they must immediately forward it to the DPO.

Children & Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests

- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs.

We will take into account whether the request is repetitive in nature when making this decision. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

Other Data Protection Rights of the Individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances) Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

Section 8: Parental Request to See the Educational Record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it. This right applies as long as the pupil concerned is aged under 18. There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

Section 9: Closed Circuit Television (CCTV)

Purpose of CCTV

The purpose of the CCTV system is to:

- Make members of the school community feel safe
- Protect members of the school community from harm to themselves or to their property
- Deter criminality in the school
- Protect school assets and buildings
- Assist police to deter and detect crime
- Determine the cause of accidents
- Assist in the effective resolution of any disputes which may arise in the course of disciplinary and grievance proceedings
- To assist in the defence of any litigation proceedings

The CCTV system will not be used to:

- Encroach on an individual's right to privacy
- Monitor people in spaces where they have a heightened expectation of privacy (including toilets and changing rooms)
- Follow particular individuals, unless there is an ongoing emergency incident occurring
- Pursue any other purposes than the ones stated above

The list of uses of CCTV is not exhaustive and other purposes may be or become relevant.

- The CCTV system is registered with the Information Commissioner under the terms of the Data Protection Act 2018.

- The system complies with the requirements of the Data Protection Act 2018 and UK GDPR. Footage or any information gleaned through the CCTV system will never be used for commercial purposes.
- In the unlikely event that the police request that CCTV footage be released to the media, the request will only be complied with when written authority has been provided by the police, and only to assist in the investigation of a specific crime.
- The footage generated by the system should be of good enough quality to be of use to the police or the court in identifying suspects.

Definitions

Surveillance: the act of watching a person or a place

CCTV: closed circuit television; video cameras used for surveillance

Covert surveillance: operation of cameras in a place where people have not been made aware they are under surveillance

Covert Surveillance

Covert surveillance will only be used in extreme circumstances, such as where there is suspicion of a criminal offence. If the situation arises where covert surveillance is needed (such as following police advice for the prevention or detection of crime or where there is a risk to public safety), a data protection impact assessment will be completed in order to comply with data protection law.

Location of Cameras

Cameras are located in places that require monitoring in order to achieve the aims of the CCTV system. Cameras are positioned in order to maximise coverage, but there is no guarantee that all incidents will be captured on camera.

Cameras are located in:

- Classrooms
- Offices
- Internal social spaces
- External social spaces

Wherever cameras are installed appropriate signage is in place to warn members of the school community that they are under surveillance.

The signage:

- Identifies the school as the operator of the CCTV system Identifies the school as the data controller

- Provides contact details for the school Cameras are not and will not be aimed off school grounds into public spaces or people's private property.

Roles & Responsibilities

The Proprietor

- The Proprietor has the ultimate responsibility for ensuring the CCTV system is operated within the parameters of this policy and that the relevant legislation is complied with.

The Headteacher

- Takes responsibility for all day-to-day leadership and management of the CCTV system
- Liaise with the data protection officer (DPO) to ensure that the use of the CCTV system is in accordance with the stated aims and that its use is needed and justified
- Ensure that the guidance set out in this policy is followed by all staff
- Review the CCTV policy to check that the school is compliant with legislation
- Ensure all persons with authorisation to access the CCTV system and footage have received proper training from the DPO in the use of the system and in data protection
- Sign off on any expansion or upgrading to the CCTV system, after having taken advice from the DPO and having taken into account the result of a data protection impact assessment
- Decide, in consultation with the DPO, whether to comply with disclosure of footage requests from third parties
- Take care of the day-to-day maintenance and operation of the CCTV system
- Oversee the security of the CCTV system and footage
- Check the system for faults and security flaws termly
- Ensure the data and time stamps are accurate termly

The Data Protection Officer

- Train persons with authorisation to access the CCTV system and footage in the use of the system and in data protection
- Train all staff to recognise a subject access request Deal with subject access requests in line with the Freedom of Information Act (2000) Monitor compliance with UK data protection law
- Advise on and assist the school with carrying out data protection impact assessments
- Act as a point of contact for communications from the Information Commissioner's Office Conduct data protection impact assessments
- Ensure data is handled in accordance with data protection legislation
- Ensure footage is obtained in a legal, fair and transparent manner
- Ensure footage is destroyed when it falls out of the retention period
- Keep accurate records of all data processing activities and make the records public on request Inform subjects of how footage of them will be used by the school, what their rights are, and how the school will endeavour to protect their personal information
- Ensure that the CCTV systems are working properly and that the footage they produce is of high quality so that individuals pictured in the footage can be identified
- Ensure that the CCTV system is not infringing on any individual's reasonable right to privacy in public spaces
- Carry out termly checks to determine whether footage is being stored accurately, and being deleted after the retention period
- Receive and consider requests for third-party access to CCTV footage

Operation of the CCTV System

- The CCTV system will be operational 24 hours a day, 365 days a year.
- The system is registered with the Information Commissioner's Office.
- The system will not record audio. Recordings will have date and time stamps.
- This will be checked by the system manager termly and when the clocks change.

Storage of CCTV Footage

- Footage will be retained for 30 days. At the end of the retention period, the files will be overwritten automatically.
- On occasion footage may be retained for longer than 30 days, for example where a law enforcement body is investigating a crime, to give them the opportunity to view the images as part of an active investigation.
- Recordings will be downloaded and encrypted, so that the data will be secure and its integrity maintained, so that it can be used as evidence if required.
- The DPO will carry out termly checks to determine whether footage is being stored accurately, and being deleted after the retention period.

Access to CCTV Footage

- Access will only be given to authorised persons, for the purpose of pursuing the aims stated in this policy, or if there is a lawful reason to access the footage.
- Any individuals that access the footage must record their name, the date and time, and the reason for access in the access log.
- Any visual display monitors will be positioned so only authorised personnel will be able to see the footage.

Staff Access

CCTV footage will only be accessed from authorised personnel's work devices, or from the visual display monitors. All members of staff who have access will undergo training to ensure proper handling of the system and footage. Any member of staff who misuses the surveillance system may be committing a criminal offence, and will face disciplinary action.

The following members of staff have authorisation to access the CCTV footage:

- **The Proprietor:** Mital Thanki
- **The Headteacher:** Katie James
- **The Business Manager**: Poonam Chamund
- **The Data Protection Officer:** Caroline Burgess
- **The System Manager:** East Midlands Security & Fire
- Anyone with express permission of the SLT and Site Leads

Subject Access Requests (SAR)

According to UK GDPR and Data Protection Act 2018, individuals have the right to request a copy of any CCTV footage of themselves.

Upon receiving the subject access request the school will immediately issue a receipt and will then respond within 1 calendar month. All staff have received training to recognise SARs.

When a SAR is received staff should inform the DPO in writing. When making a request, individuals should provide the school with reasonable information such as the date, time and location the footage was taken to aid school staff in locating the footage.

On occasion the school will reserve the right to refuse a SAR, if, for example, the release of the footage to the subject would prejudice an ongoing investigation. Images that may identify other individuals need to be obscured to prevent unwarranted identification.

The school will attempt to conceal their identities by blurring out their faces, or redacting parts of the footage. If this is not possible the school will seek their consent before releasing the footage. If consent is not forthcoming the still images may be released instead.

The school reserves the right to charge a reasonable fee to cover the administrative costs of complying with a SAR that is repetitive, unfounded or excessive.

Footage that is disclosed in a SAR will be disclosed securely to ensure only the intended recipient has access to it.

Records will be kept that show the date of the disclosure, details of who was provided with the information (the name of the person and the organisation they represent), and why they required it.

Individuals wishing to make an SAR can find more information about their rights, the process of making a request, and what to do if they are dissatisfied with the response to the request on the ICO website.

Third Party Access

CCTV footage will only be shared with a third party to further the aims of the CCTV system:

- Footage will only ever be shared with authorised personnel such as law enforcement agencies or other service providers who reasonably need access to the footage (e.g. investigators).
- All requests for access should be set out in writing and sent to the headteacher and the DPO. The school will comply with any court orders that grant access to the CCTV footage. The school will provide the courts with the footage they need without giving them unrestricted access.
- The DPO will consider very carefully how much footage to disclose, and seek legal advice if necessary. The DPO will ensure that any disclosures that are made are done in compliance with UK GDPR.
- All disclosures will be recorded by the DPO.

Data Protection Impact Statement (DPIA)

The school follows the principle of privacy by design. Privacy is taken into account during every stage of the deployment of the CCTV system, including its replacement, development and upgrading.

The system is used only for the purpose of fulfilling its aims.

When the CCTV system is replaced, developed or upgraded a DPIA will be carried out to be sure the aim of the system is still justifiable, necessary and proportionate.

The DPO will provide guidance on how to carry out the DPIA.

The DPIA will be carried out by the Proprietor and Safeguarding Lead.

Those whose privacy is most likely to be affected, including the school community and neighbouring residents, will be consulted during the DPIA, and any appropriate safeguards will be put in place.

A new DPIA will be done annually and/or whenever cameras are moved, and/or new cameras are installed. If any security risks are identified in the course of the DPIA, the school will address them as soon as possible.

Security

The system manager will be responsible for overseeing the security of the CCTV system and footage. The system will be checked for faults once a term . Any faults in the system will be reported as soon as they are detected and repaired as soon as possible, according to the proper procedure. Footage will be stored securely and encrypted wherever possible The CCTV footage will be password protected and any camera operation equipment will be securely locked away when not in use. Proper cyber security measures will be put in place to protect the footage from cyber-attacks. Any software updates (particularly security updates) published by the equipment's manufacturer that need to be applied, will be applied as soon as possible.

Complaints

Complaints should be directed to the Headteacher or the DPO and should be made according to the school's Complaints Procedure Policy.

Monitoring

The policy will be reviewed annually by the DPO/DSL to consider whether the continued use of a surveillance camera remains necessary, proportionate and effective in meeting its stated purposes.

Section 10: Photographs & Videos

As part of our school activities, we may take photographs and record images of individuals within our school. We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Where the school takes photographs and videos, uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Section 11: Data Protection by Design & Default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices

- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply

Maintaining records of our processing activities, including:

- For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
- For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

Section 12: Data Security & Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff or pupils who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

Section 13: Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Section 14: Personal Data Breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix A.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

Refer to Appendix A & B

Section 15: Training

All staff are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

Section 16: Data Retention

Core Principles

Spark is committed to handling all records in line with the principles of the UK GDPR and the Data Protection Act 2018, specifically:

- Lawfulness, fairness, transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

This retention schedule sets out how long different types of records will be kept before secure destruction or anonymisation. It ensures compliance with statutory guidance, including the latest *Keeping Children Safe in Education* the Independent School Standards, health and safety law, employment law, HMRC requirements, and safeguarding best practice.

Where records are kept beyond the minimum statutory period (e.g. safeguarding files), this is justified by the need to protect children and manage potential future legal claims.

Secure Disposal

- Paper records are shredded or incinerated.
- Digital records are securely deleted from all devices, backups, and cloud systems.
- For safeguarding files, a record of disposal (date and method) is kept.

Oversight

- The **Data Protection Officer (DPO)** is responsible for ensuring compliance with this schedule.
- The **Headteacher** monitors adherence operationally.
- The **Proprietor** provides overall oversight and approves any exceptions.

Refer to Appendix C: Data Retention Schedule

Section 17: Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed annually and approved by the **Headteacher.**

Appendix A: Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the data protection officer (DPO).

The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people
- Staff will cooperate with the investigation (including allowing access to information and responding to questions).

The investigation will not be treated as a disciplinary investigation

- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the Headteacher and the Proprietor

The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)

- The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
- The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the schools computer system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach.

As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible: The categories and approximate number of individuals concerned and the categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach

- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing.

This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO.

For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals) Records of all breaches will be stored on the school's computer system.
- The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible
- The DPO and Headteacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Appendix B: Actions to Minimise the Impact of Data Breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information.

We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the external IT support provider to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO and IT support will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners

Other types of breach could include:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with Proprietor
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- Hardcopy reports sent to the wrong pupils or families

Appendix C: Data Retention Schedule

Table A: Pupil Records				
Record Type	Retention	Trigger	Responsible	Notes (legal/sector basis)
Pupil educational record (if final school)	DOB + 31 years	Pupil DOB	Headteacher / DPO	EHCP cohort → use SEN anchor. Transfer securely if pupil moves.
Safeguarding / child protection file	DOB + 31 years	Pupil DOB	DSL / DPO	Baseline is DOB + 25; EHCP cohort → DOB + 31. Keep transfer receipt; don't retain duplicate file after transfer.
Low level concerns (re staff) about conduct towards a pupil	Staff leaves + 6 years	Staff end date	Headteacher / DPO	Keep separately from pupil file; pattern-spotting per KCSIE. If escalated → follow safeguarding retention above.
LAC / PEP documents (school copy)	DOB + 31y ears	Pupil DOB	DSL / DPO	LA holds statutory care record for 75 years; your copy follows EHCP anchor.
SEN/EHCP (plans, reviews, provision)	DOB + 31 yeas	Pupil DOB	DSL / DPO	IRMS: SEN records 31 years.
Exclusions / serious behaviour	DOB + 31 yeas	Pupil DOB	Headteacher / DPO	Extended retention prudent for claims; justified in policy. (IRMS rationale re Limitation Act).
Assessments / Internal results	6 years after leaving	Leaving date	Headteacher/DPO	Keep anonymised analytics longer if needed.
Exam scripts/coursework (school-held)	Exam series + 1 yr (or until appeals conclude)	Exam Date	Headteacher	Follow JCQ; then secure disposal.

Exam certificates (unclaimed)	Hold **12 months** then destroy; keep destruction **log 4 yrs**	Issue date	Headteacher	JCQ notice to centres.
Trip Consent (no incident)	Trip + **1 yr**	Trip end	DSL / Headteacher	If any incident → see next row.
Trip incident / first aid / H&S on trip	DOB + 31	Pupil DOB	DSL / Headteacher	Align to safeguarding/EHCP anchor for pupil-specific incidents.
Medical (care plans, meds consent)	**DOB + 25** (or + **31** if tied to EHCP dispute)	Pupil DOB	Headteacher/Medical lead	NHS/sector norm is 25; where clearly linked to SEND disputes, justify **31**
Photography & image consents	Until pupil leaves **or** consent withdrawn	Event/leaving	DPO	Remove images when consent ends unless other lawful basis.
Table B: Staff & Safer Recruitment				
Personnel file (contract, appraisal)	End of employment + **6 yrs**	Staff end date	SBM/DPO	Limitation Act.
SCR (current staff)	Live; **archive 6 yrs** post-employment	Staff end date	SBM/DPO	Don't keep historic DBS cert copies.
DBS evidence	Record check/date only; **no cert copy**	Check date	SBM/DPO	DBS Code; KCSIE.
Right-to-work	**2 yrs** post-employment	Staff end date	SBM	Home Office.
References (successful)	**On personnel file**	Staff end date	SBM	
Applications & interview notes (unsuccessful)	**6 months**	Offer filled	SBM	GDPR fairness.
Allegations against staff (non-malicious)	**To retirement age or 10 yrs (whichever longer)**	Case close	Headteacher/DPO	KCSIE retention. Malicious → remove.
Training (safeguarding/Prevent/Team-Teach, etc.)	**Employment + 6 yrs**	Staff end date	DSL/SBM	Inspectors check historic compliance.

Table C: Governance, Finance & Business				
Proprietor/board minutes	Permanent	Meeting date	Proprietor/Clerk	ISS Part 8 evidence.
Register of interests / s128 checks	Tenure + 6 yrs	End of tenure	SBM	
Complaints (general)	6 yrs	Case close	Headteacher	ISS Part 7.
Complaints (safeguarding-related)	DOB + 31	Pupil DOB	DSL/DPO	
Annual safeguarding audits / proprietor monitoring	6 yrs	Report date	DSL/Proprietor	ISS/KCSIE evidence.
Budgets, accounts, invoices, expenses	6 yrs	FY end	Proprietor / SBM	HMRC/Companies Act.
Funding agreements (LA/ESFA)	Permanent or 6 yrs after cessation	Cessation	Proprietor/SBM	
Contracts with suppliers	6 yrs after end	Contract end	SBM	
Insurance policies / claims	Policy + 6 years (liability often 40 years)	End/claim close	SBM	Keep abuse-related indefinitely if advised.
Table D: Health, Safety & Premises				
Accident/incident (pupils)	DOB + 31	Pupil DOB	Proprietor	RIDDOR + EHCP anchor.
Accident/incident (staff)	6–7 yrs (serious → 40 yrs)	Incident date	Proprietor	
Risk Assessments	3 yrs after superseded	Superseded	Proprietor	
Fire safety logs/drills	3 yrs	Entry date	Proprietor	
Asbestos register	Lifetime of building +	Ongoing	Proprietor	Typically 40 yrs minimum.
Legionella/water tests	6 yrs	Entry date	Proprietor	HSE
COSHH	40 years	Exposure date	Proprietor	
Table E: ICT, Online Safety & Security				
Filtering & monitoring: log of checks (who/when/what)	≥ 6 months (per NCSC); longer if risk assessment requires	Check date	DSL/ Kazzoo	DfE requires keeping logs; keep longer where prudent. Incidents linked to pupils → DOB + 31.

Security/audit logs (staff access)	≥ 6 months (critical logs), up to 12 months	Log date	IT/DPO	Based on risk; extend if investigation.
CCTV	~30 days, unless incident	Recording date	DPO/Proprietor	ICO norm; incident footage kept until conclusion of case (then per anchor above
Data breaches register	6 yrs	Entry date	DPO	ICO audits.