GDPR Data Protection Policy

Reviewed: November 2024
Next review: November 2025
Ratified by Committee – November 2024

Statement of Intent

Stepping Stones School is required to keep and process certain information about its pupils staff, parents or carers and other individuals who come into contact with the school. This is in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially children's services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the school complies with the following core principles of the GDPR. All staff are involved with and have responsibility for the collection, processing and disclosure of personal data and must be aware of their duties and responsibilities by adhering to this policy and the law.

Organisational methods for keeping data secure are imperative, and Stepping Stones School believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy complies with the requirements set out in the GDPR, which came into effect on 25 May 2018. The government confirmed that the UK's decision to leave the EU does not affect compliance with GDPR.

The Data Protection Officer is the School Business Manager and can be contacted by the school telephone number 01524 67164 or email bursar@steppingstones.lancs.sch.uk
road.lancs.sch.uk

Appendix A – Data Protection Impact Assessment
Appendix B – Breach Report Form
Appendix C – Security and Breach Management Plan
Appendix D – Photos and Videos in School
Appendix E – Data Retention Schedule (IRMS Version 6)

Review

This policy will be reviewed regularly.

Policy approved by the Full Governing Body on November 2024

Signed: Michael Hooper (Headteacher)

Legal framework

This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR) May 2018
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection Regulations 2004
- The School Standards and Framework Act 1998

This policy will also have regard to guidance from the Information Commissioner's Office.

Information Commissioner's Office membership valid June 2024

Other School Policies Relating to GDPR Data Protection

Staff (including Volunteers and Agency Workers) should also refer to the following polices in relation to GDPR Data Protection:

- Child Protection and Safeguarding
- E Safety and ICT Security Policy
- Staff Code of Conduct including Agency Staff
- Non-Disclosure and Confidentiality Agreement
- Governors Code of Conduct
- Volunteer in School Policy
- Complaints Policy
- PSHE
- Freedom of Information Access
- National Curriculum
- School Admissions
- Staff Disciplinary and Grievance
- Special Educational Needs
- Whistleblowing by an Employee (Included the School Finance Manual)

Types of Data

For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

Sensitive personal data is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health and social matters.

1. Principles

In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data which is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

2. Accountability

Stepping Stones School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

The school will provide comprehensive, clear and transparent privacy policies.

Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

The school will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation.
- Pseudonymisation.
- Transparency.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

Data protection impact assessments will be used, where appropriate.

3. Data Protection Officer (DPO)

A DPO will be appointed in order to:

- Inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws.

- Monitor the school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools.

The DPO will report to the highest level of management at the school, which is the Headteacher.

The DPO will operate independently and will not be dismissed or penalised for performing their task.

Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

The DPO will work with the Governing Body to audit and report on DP

4. Lawful processing

The legal basis for processing data will be identified and documented prior to data being processed.

Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for:
  - Compliance with a legal obligation.
  - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
  - For the performance of a contract with the data subject or to take steps to enter into a contract.
  - Protecting the vital interests of a data subject or another person.
  - For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the school in the performance of its tasks.)

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by law.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
  - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
  - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
  - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
  - Reasons of substantial public interest on the basis of law which is proportionate to the aim pursued and which contains appropriate safeguards.
  - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee and medical diagnosis.
  - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
  - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

5. Consent

Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes. The Primary contact on SIMS will be used for consent of pupil data.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

Where consent is given, a record will be kept documenting how and when consent was given.

The school ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

Consent can be withdrawn in writing by the individual at any time.

For all pupils at Stepping Stones School, up to and including Year 6, parental consent will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

6. The right to be informed

The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge. The Privacy Notices for Parents and Pupils are published on the school website. The Parent Privacy Notice is issued to parents on admission of the pupil. Staff are issued with the Privacy Notice during induction with the School Business Manager.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller (and where applicable, the controller's representative) and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
  - Withdraw consent at any time.
  - Lodge a complaint with a supervisory authority.
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

In relation to data that is not obtained directly from the data subject, this information will be supplied:
- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

7. The right of access

Individuals have the right to obtain confirmation that their data is being processed.

Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing. The school will centrally record all SARs whether in writing or verbally. A SAR is different to Freedom of Information – please refer to FOI statement.

The school will verify the identity of the person making the request before any information is supplied.
A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within one month of receipt.

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

8. The right to rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified.

Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.

Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

9. The right to erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed for the offer of information society services to a child

The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- Legal compliance with completing a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific and/or historical research or statistical purposes
- The exercise or defence of legal claims

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.
Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

10. The right to restrict processing

Individuals have the right to block or suppress the school's processing of personal data.

In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

The school will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
- Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

The school will inform individuals when a restriction on processing has been lifted.

11. The right to data portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

Personal data will be provided in a structured, commonly used and machine-readable form.

The school will provide the information free of charge.

Where feasible, data will be transmitted directly to another organisation at the request of the individual.

The school is not required to adopt or maintain processing systems which are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual.

The school will respond to any requests for portability within one month.

Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

12. The right to object

The school will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- The school will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above, but is carried out online, the school will offer a method for individuals to object online.

13. Automated decision making and profiling

School does not engage with automated decision making and or profiling. This ensures that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of a decision and challenge it.

14. Privacy by design and privacy impact assessments

The school will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into processing activities.

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy. The originator/person leading a new project for IT software/platform/application, or other system relating to data usage, is to complete the template DPIA – see Appendix A. On completion the assessment is to be emailed to the DPO for checking. New systems or procedures which include staff or pupil data must not be used until the DPIA is finalised by the DPO.

DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur.

Where a DPIA indicates high risk data processing, the DPO will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

15. Data breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The Headteacher will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their induction and CPD training.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it.

The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly.

A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Effective and robust breach detection, investigation and internal reporting procedures are in place at the school, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach and action taken

- A description of the proposed measures to be taken to deal with the personal data breach

Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

The breach report form can be found at Appendix B and the Security Breach Prevention and Management Plan at Appendix C. The form is to be completed by staff and handed immediately to the DPO who will then decide further steps eg refresher training. The DPO will enter the breach and subsequent action on the Breach Log for School.

16. Data security

Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

Confidential paper records will not be left unattended or in clear view anywhere with general access.

Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

All electronic devices are password-protected to protect the information on the device in case of theft. Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.

Staff will not use their personal I Pads, pen drives, laptops or computers for school purposes.

Governors are to ensure that school documents are not retained with personal and identifiable data. Their home computers and laptops are to have passwords and checked for encryption.

All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

When sending confidential information by email, staff will always check that the recipient is correct before sending.

Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data. Each class are provided with a Confidential Red Wallet which has a break clip to ensure non-tamper. Additional wallets and clips can be obtained from the DPO.

Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.

The physical security of the school's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

Stepping Stones School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

17. Publication of information

Stepping Stones School has a publication scheme outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Annual reports
- Financial information

Classes of information can be made available quickly and easily on request.

Stepping Stones School will not publish any personal information, including photos, on its website without the permission of the affected individual.

When uploading information to the school website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

18. CCTV and photography

The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles. Consent is requested and recorded for all members of staff, governors and pupils.

The school uses photographs of pupils to promote the learning within school and communicate to stakeholders. Staff will check permission and confirm prior to publishing photographs or videos.

Precautions, as outlined in Appendix C Photography and Videos at School, are taken when publishing photographs of pupils, in print, video or on the school website.

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR. Parents are reminded to photograph or video their own child only and exclude all other children, unless they have agreement from other parents eg friendship groups.

The school does not collect CCTV images. There is CCTV covering the playground area, which is maintained by Moorside Primary School and is only switched on in the evening due to Anti-social behaviour in the area.

.

19. Data retention

Data will not be kept for longer than is necessary and in line with the IRMS Retention Schedule – see Appendix E

Unrequired data will be deleted as soon as practicable.

Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

Staff are to termly check their folders on the computer drives for unrequired and unlawful data, such as photos of ex pupils and staff.

20. DBS data

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

Copies of DBS certificates will not be retained within staff files.

Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

Privacy Impact Assessments

Privacy impact assessments (PIAs) allow schools to consider the privacy issues relating to any personal information used within its projects.

A PIA will allow schools to identify and fix problems at an early stage.

A PIA should be completed by a member of staff who has responsibility for the processing of the project information.

The Information Commissioners Office provide guidance on:
https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

PRIVACY IMPACT ASSESSMENT

Step one: About the project

What is the project name?	
What are the project objectives?	
Is there a project manager?	
Who are the customers?	
Who are the stakeholders?	
How long is the project due to last?	
What benefits will the project bring to the school, individuals and to other parties?	
What personal information is being used? Name, address, NI number, date of birth, gender, religion, occupation, medical history, ethnic origin, other?	
What is your legal basis for processing this information? • Consent • Legal Obligation • Contract • Vital Interests • Public Interest	

Step two: Describe the information flows

If you are using consent, how are you collecting the data subjects consent to process their personal information?	
What information are you collecting from the data subject?	
How will the information be collected?	
How will the information be used?	
Who will the information be shared with?	
If the information will be shared with suppliers, do we have a contract in place with the supplier?	
If the information will be shared with partners, do we have an information sharing agreement in place?	
Who will have access to the information?	
How long will the information be retained?	
How and when will the information deleted?	

Step three: Identify the privacy and related risks

Are there any risks to individual's privacy?	
Are there any risks to compliance with the law e.g. Data Protection Act, GDPR, PECR, Human Rights Act.	
Are there any risks to the school's reputation or finances?	
How will you check that the personal information used is accurate and complete?	
Have you set a retention period so that the information is not kept longer than necessary?	

Is the information being stored securely?	
Is the information being transferred to another country?	

Step four: Identify privacy solutions

Please list any risks and mitigating actions below.

Repeat the following for each risk.

Risk ID	Unique project risk id
Risk Description	[Event that has an effect on objectives] **caused by** [cause/s] **resulting in** [consequence/s]. 1. What could happen (event) 2. Why could it happen (caused by) 3. Resulting in (consequences)
Risk Type	• Political • Economic • Social • Technological • Legal • Environmental • Democratic • Organisational
Possible Consequences	What could happen if no action was taken to control the risk?
Current Situation	What is the current situation before any mitigating actions are taken?
Current Risk Score	Risk Score = likelihood x Impact.
Mitigating Actions	What mitigating actions are you taking to reduce the risk?
Residual Risk Score (after mitigating actions)	Risk Score = likelihood x Impact.
Risk Owner	Who owns the risk?
Direction of Travel	What is the direction of travel? Upwards or downwards or static.

How to score your risks

	CATASTROPHIC	5	10	**15**	**20**	**25**
	MAJOR	4	8	**12**	**16**	**20**
	MODERATE	3	6	9	**12**	**15**
IMPACT	MINOR	2	4	6	8	10
	INSIGNIFICANT	1	2	3	4	5
LIKELIHOOD		RARE	UNLIKELY	POSSIBLE	LIKELY	CERTAIN

Step five: Sign off

Privacy risks and mitigating actions approved by|:

- Name:
- Signature:
- Date:

Step six: Integrate these risks and mitigating actions back into the project plan and review at each project meeting

APPENDIX B

STEPPING STONES SCHOOL- BREACH OF DATA PROTECTION REPORT- CONFIDENTIAL

On completion, pass form to the DPO (School Business Manager) immediately

Report completed by : _____ Date: _____

Date of Breach:
Number of people affected:
Type of Breach:
Breach made by:
Description of breach:
How did the school become aware of the breach:
Who became aware of the breach:
Date on which the school became aware of the breach:
Consequences of the breach:
Action Taken:
Affected people informed:
Raised to the ICO and Date:
IF no, why not?:
If raised, by who:
Further training/action required:

Security Breach Prevention and Management Plan

Statement of intent

Stepping Stones School is committed to maintaining the confidentiality of its information and ensuring that the details of the finances, operations and individuals within the school are only accessible by the appropriate individuals. It is therefore important to uphold high standards of security, take suitable precautions, and to have systems and procedures in place that support this.

The school recognises, however, that breaches in security can occur, particularly as the majority of information is stored online or on electronic devices which are increasingly vulnerable to cyber-attacks. This being the case, it is necessary to have a contingency plan containing procedures to minimise the potential negative impacts of any security breach, to alert the relevant authorities, and to take steps to help prevent a repeat occurrence.

For the purposes of this policy, the title of '**data controller**' will be used in reference to the person(s) primarily responsible for the handling and protection of information and data within a school.

1. Types of security breach and causes

Unauthorised use without damage to data – involves unauthorised persons accessing data on the school system, e.g. 'hackers', who may read the data or copy it, but who do not actually damage the data in terms of altering or deleting it.

Unauthorised removal of data – involves an authorised person accessing data, who removes the data to pass it on to another person who is not authorised to view it, e.g. a staff member with authorised access who passes the data on to a friend without authorised access – this is also known as data theft. The data may be forwarded or deleted altogether.

Damage to physical systems – involves damage to the hardware in the school's ICT system, which may result in data being inaccessible to the school and/or becoming accessible to unauthorised persons.

Unauthorised damage to data – involves an unauthorised person causing damage to data, either by altering or deleting it. Data may also be damaged by a virus attack, rather than a specific individual.

Breaches in security may be caused as a result of actions by individuals, which may be accidental, malicious or the result of negligence – these can include:

Accidental breaches, e.g. as a result of insufficient training for staff, so they are unaware of the procedures to follow.

Malicious breaches, e.g. as a result of a hacker wishing to cause damage to the school through accessing and altering, sharing or removing data.

Negligence, e.g. as a result of an employee that is aware of school policies and procedures, but disregards these.

Breaches in security may also be caused as a result of system issues, which could involve incorrect installation, configuration problems or an operational error – these can include:

Incorrect installation of anti-virus software and/or use of software which is not the most up-to-date version, meaning the school software is more vulnerable to a virus

Incorrect firewall settings are applied, e.g. access to the school network, meaning individuals other than those required could access the system

Confusion between backup copies of data, meaning the most recent data could be overwritten

2. Roles and responsibilities

The Headteacher is responsible for implementing effective strategies for the management of risks posed by internet use, and to keep its network services, data and users secure.

The Data Protection Officer (SBM) is responsible for the overall monitoring and management of data security. Also responsible for establishing a procedure for managing and logging incidents.

The Governing Body is responsible for strategic compliance of data protection.

All members of staff and pupils are responsible for adhering to the processes outlined in this and the GDPR policy, alongside the school's E-Safety Policy and Acceptable Use Policy.

Secure configuration

An inventory/asset register will be kept of all IT hardware and software currently in use at the school, including mobile phones and other personal devices provided by the school. This will be stored in the school systems and will be audited on an annual basis to ensure it is up-to-date.

Any changes to the IT hardware or software will be documented using the register.

IT support within school will audit regularly to ensure the software is up-to-date. Any new versions of software or new security patches will be added to systems, ensuring that they do not affect network security, and is to be recorded.

Any software that is out-of-date or reaches its 'end of life' will be removed from systems, i.e. when suppliers end their support for outdated products such that any security issues will not be rectified.

All hardware, software and operating systems will require passwords for individual users before use. Passwords will be changed on a termly basis to prevent access to facilities which could compromise network security.

The school believes that locking down hardware, such as through the use of strong passwords, is an effective way to prevent access to facilities by unauthorised users.

3. Network security

The school will employ firewalls in order to prevent unauthorised access to the systems. The school's firewall will be deployed as a **Centralised deployment**: the broadband service connects to a firewall that is located within a data centre or other major network location. Any compromise of security through the firewall will be reported to the DPO.

4. Malware prevention

The school understands that malware can be damaging for network security and may enter the network through a variety of means, such as email attachments, social media, malicious websites or removable media controls.

The IT co-ordinator will ensure that all school devices have secure malware protection and undergo regular malware scans. The IT co-ordinator will update malware protection on a regular basis to ensure it is up-to-date and can react to changing threats.

Malware protection will also be updated in the event of any attacks to the school's hardware and software.

Filtering of websites, as detailed in section 7 of this policy, will ensure that access to websites with known malware is blocked immediately and reported to the DPO (SBM).

Staff must be vigilant regarding malware that is transmitted by email. Caution is to be used with regard to spam or other messages which are designed to exploit users.

The IT co-ordinator will review the mail security technology on a regular basis to ensure it is kept up-to-date and effective.

5. User privileges

The school understands that controlling what users have access to is important for promoting network security. User privileges will be differentiated, i.e. pupils will have different access to data and the network than members of staff.

The IT co-ordinator will ensure that user accounts are set up to allow users access to the facilities required, in line with the DPO and Headteacher's instructions, whilst minimising the potential for deliberate or accidental attacks on the network.

The IT co-ordinator will ensure that websites are filtered for inappropriate and malicious content. Any member of staff or pupil that has accessed inappropriate or malicious content will be recorded in accordance with the monitoring process in section 12 of this policy.

All users will be required to change their passwords on a regular basis and must ensure that passwords are strong. Users will also be required to change their password if they become known to other individuals. Pupils are responsible for remembering their passwords; however, the IT co-ordinator will have an up-to-date record of all usernames and passwords, and will be able to reset them if necessary.

Pupils in KS1 will not have individual logins, and class logins will be used instead. If it is appropriate for a pupil to have an individual login, the IT co-ordinator will set up their individual user account, ensuring appropriate access and that their username and password is recorded.

Only individual accounts will be used for staff and older students.

The IT co-ordinator will manage this provision to ensure that all users are up to date and deleted when leaving school so that they do not have access to the system.

The IT co-ordinator will review the system on a regular basis to ensure the system is working at the required level.

6. Monitoring usage

Monitoring user activity is important for the early detection of attacks and incidents, as well as inappropriate usage by pupils or staff.

The school will inform all pupils and staff that their usage will be monitored, in accordance with the school's Acceptable Use Policy and E-Safety Policy.

If a user accesses inappropriate content or a threat is detected, an alert will be sent to the data controller. Alerts will also be sent for unauthorised and accidental usage.

Alerts will identify: the user, the activity that prompted the alert and the information or service the user was attempting to access.

All incidents will be responded to in accordance with this policy, and as outlined in the E-Safety Policy and Staff Disciplinary Policy.

7. Removable media controls and home working

The school understands that pupils and staff may need to access the school network from areas other than on the premises. Effective security management will be established to prevent access to, or leakage of, data, as well as any possible risk of malware.

The IT co-ordinator will encrypt all school-owned devices for personal use, such as laptops, USB sticks, mobile phones and tablets, to ensure that they are password protected. If any portable devices are lost, this will prevent unauthorised access to personal data.

Pupils and staff are not permitted to use their personal devices where the school shall provide alternatives, such as work laptops, tablets and USB sticks, unless instructed otherwise by the Headteacher.

If pupils and staff are instructed that they are able to use their personal devices, they will ensure that they have an appropriate level of security and firewall to prevent any compromise of the school's network security. This can be checked by the IT co-ordinator.

When using laptops, tablets and other portable devices, the Headteacher will determine the limitations for access to the network, as described in section 5 of this policy.

Staff who use school-owned laptops, tablets and other portable devices will use them for work purposes only, whether on or off school premises.

The IT co-ordinator will use encryption to filter the use of websites on these devices, in order to prevent inappropriate use and external threats which may compromise network security when bringing the device back onto the premises.

The school uses tracking technology where possible to ensure that lost or stolen school devices can be retrieved.

All data will be held on systems centrally in order to reduce the need for the creation of multiple copies, and/or the need to transfer data using removable media controls.

The Wi-Fi network at the school will be password protected and will only be given out as required. Staff and pupils are not permitted to use the Wi-Fi for their personal devices, such as mobile phones or tablets, unless instructed otherwise by the Headteacher.

8. Backing-up data

Back-ups are run overnight and are completed before the beginning of the next school day.

Upon completion of back-ups, data is stored externally by the schools IT third party support.

Only authorised personnel are able to access the school's data.

9. User training and awareness

The DPO will inform staff of network drives and passwords on their induction. New staff are to complete the online GDPR Training. All staff are to complete the DP online training annually.

Training for all staff members will be arranged by the Data Protection Officer within two weeks following an attack or significant update.

Through training, all pupils and staff will be aware of who they should inform first in the event that they suspect a security breach, and who they should inform if they suspect someone else is using their passwords.

All users will be made aware of the disciplinary procedures for the misuse of the network leading to malicious attacks, in accordance with the process detailed in the E-Safety Policy.

10. Security breach incidents

Any individual that discovers a security data breach will report this immediately to the Data Protection Officer (SBM) using the Data Breach Report Form at Appendix B

The school's DPO will take the lead in investigating the breach, and will be allocated the appropriate time and resources to conduct this. The DPO, as quickly as reasonably possible, will ascertain the severity of the breach and determine if any personal data is involved or compromised. The DPO will oversee a full investigation and produce a comprehensive report. The cause of the breach, and whether or not it has been contained, will be identified – ensuring that the possibility of further loss/jeopardising of data is eliminated or restricted as much as possible.

If the DPO determines that the severity of the security breach is low, the incident will be managed in accordance with the following procedures:

In the event of an internal breach, the incident is recorded using an incident log, and by identifying the user and the website or service they were trying to access.

The Headteacher will issue disciplinary sanctions to the pupil or member of staff, in accordance with the processes outlined in the E-safety Policy.

The DPO will work with the third-party provider to provide an appropriate response to the attack, including any in-house changes. Any further action which could be taken to recover lost or damaged data will be identified – this includes the physical recovery of data, as well as the use of back-ups. Where the security risk is high, the school will establish what steps need to be taken to prevent further data loss which will require support from various school departments and staff.

This action will include:

Informing the ICO
Informing relevant staff of their roles and responsibilities in areas of the containment process.
Taking systems offline.
Retrieving any lost, stolen or otherwise unaccounted for data.
Restricting access to systems entirely or to a small group.
Backing up all existing data and storing it in a safe location.
Reviewing basic security, including:
Changing passwords and login details on electronic equipment.
Ensuring access to places where electronic or hard data is kept is monitored and requires authorisation.

Where appropriate, e.g. if offences have been committed under the Computer Misuse Act 1990, the DPO will inform the police of the security breach. The DPO will arrange for testing of all systems to ensure they are functioning normally, and the incident will only be deemed 'resolved' when it has been assured that the school's systems are safe to use.

11. Assessment of risks

The following questions will be considered by the DPO in order to fully and effectively assess the risks that the security breach has brought, and to help take the next appropriate steps. All relevant questions will be clearly and fully answered in the data controller's report and records:

- What type and how much data is involved?
- How sensitive is the data? Sensitive data is defined in the GDPR 2018; some data is sensitive because of its very personal nature (e.g. health records) while other data types are sensitive because of what might happen if it is misused (e.g. bank account details).

- Is it possible to identify what has happened to the data – has it been lost, stolen, deleted or tampered with?
- If the data has been lost or stolen, were there any protective measures in place to prevent this, such as data and device encryption?
- If the data has been compromised, have there been effective measures in place that have mitigated the impact of this, such as the creation of back-up tapes and spare copies?
- Has individuals' personal data been compromised – how many individuals are affected?
- Who are these individuals – are they pupils, staff, governors, volunteers, stakeholders, suppliers?
- Could their information be misused or manipulated in any way?
- Could harm come to individuals? This could include risks to the following:
- Physical safety
- Emotional wellbeing
- Reputation
- Finances
- Identity
- Private affairs becoming public
- Are there further implications beyond the risks to individuals? Is there a risk of loss of public confidence/damage to the school's reputation, or risk to the school's operations?
- Who could help or advise the school on the breach? Could the LA, external partners, authorities, or others provide effective support?

In the event that the DPO, or other persons involved in assessing the risks to the school, are not confident in the risk assessment, they will seek advice from the Information Commissioner's Office (ICO).

12. Consideration of further notification

The school will consider whether there are any legal, contractual or regulatory requirements to notify individuals or organisations that may be affected or who will have an interest in security.

The school will assess whether notification could help the individual(s) affected, and whether individuals could act on the information provided to mitigate risks, e.g. by cancelling a credit card or changing a password.

If a large number of people are affected, or there are very serious consequences, the ICO will be informed.

The school will consider who to notify, what to tell them and how they will communicate the message, which may include:

- A description of how and when the breach occurred and what data was involved. Details of what has already been done to respond to the risks posed by the breach will be included.
- Specific and clear advice on the steps they can take to protect themselves, and what the school is willing to do to help them.
- A way in which they can contact the school for further information or to ask questions about what has occurred.

The school will consult the ICO for guidance on when and how to notify them about breaches. The school will consider, as necessary, the need to notify any third parties – police, insurers, professional bodies, funders, trade unions, website/system owners, banks/credit card companies – who can assist in helping or mitigating the impact on individuals.

Under the GDPR, the following steps will be taken if a breach of personal data occurs:

The school will notify the ICO within 72 hours of a breach where it is likely to result in a risk to the rights and freedoms of individuals. Where a breach is likely to result in significant risk to the rights and freedoms of individuals, the school will notify those concerned directly with the breach.

Where the breach compromises personal information, the notification will contain:

- The nature of the personal data breach including, where possible:
- The type(s), e.g. staff, pupils or governors, and approximate number of individuals concerned.
- The type(s) and approximate number of personal data records concerned.
- The name and contact details of the DPO or other person(s) responsible for handling the school's information.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed, to deal with and contain the breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

13. Evaluation and response

The DPO will establish the root of the breach, and where any present or future risks lie.

The DPO will consider the data and contexts involved.

The DPO and Headteacher will identify any weak points in existing security measures and procedures.

The DPO and Headteacher will identify any weak points in levels of security awareness and training.

The DPO will report on findings and, with the approval of the school leadership team, implement the recommendations of the report after analysis and discussion.

Timeline of Incident Management

Date	Time	Activity	Decision	Name/position	Date

Photography and Videos at School

Statement of intent

At **Stepping Stones School**, we use imagery and videos for a variety of purposes, including prospectuses, display boards, educational purposes, conferences and the school website. We understand that parents may also wish to take videos or photos of their children participating in school events for personal use.

Whilst we recognise the benefits of photography and videos to our school community, we also understand that these can have significant risks for those involved. Under the legal obligations of the General Data Protection Regulation (GDPR), the school has specific responsibilities in terms of how photos and videos are taken, stored and retained.

The school has implemented a policy on the safe use of cameras and videos by staff and parents to reflect the protective ethos of the school with regard to pupils' safety.

In order to ensure that, as far as possible, the use of photography and video is used safely at all times, the policy provided below should be followed. This policy is applicable to all forms of visual media, including film, print, video, DVD and websites.

Definitions

For the purpose of this policy:

"Personal use" of photography and videos is defined as the use of cameras to take images and recordings of children by relatives, friends or known individuals, e.g. a parent taking a group photo of their child and their friends at a school event. These photos and videos are only for personal use by the individual taking the photo, and are not intended to be passed on to unknown sources. The principles of the GDPR do not apply to images and videos taken for personal use.

"Official school use" is defined as photography and videos which are used for school purposes, e.g. for building passes. These images are likely to be stored electronically alongside other personal data. The principles of the GDPR apply to images and videos taken for official school use.

"Media use" is defined as photography and videos which are intended for a wide audience, e.g. photographs of children taken for a local newspaper. The principles of the GDPR apply to images and videos taken for media use.

Staff may also take photos and videos of pupils for **"educational purposes**". These are not intended for official school use, but may be used for a variety of reasons, such as school displays, special events, assessment and workbooks. The principles of the GDPR apply to images and videos taken for educational purposes.

1. Roles and responsibilities

The Headteacher is responsible for:

- Liaising with social workers to gain consent for photography and videos of LAC pupils.
- Liaising with the data protection officer (DPO), to ensure there are no data protection breaches.
- Informing relevant bodies of any known changes to a pupil's security, e.g. child protection concerns, which would mean that participating in photography and video recordings would put them at significant risk.

- Submitting consent forms to parents with regards to photographs and videos being taken whilst at school.
- Ensuring that all photos and videos are stored and disposed of correctly, in line with the GDPR.
- Deciding whether parents are permitted to take photographs and videos during school events.
- Communicating this policy to all the relevant staff members and the wider school community, such as parents.

Parents are responsible for:

- Completing the Consent Form.
- Informing the school in writing where there are any changes to their consent.
- Acting in accordance with this policy.

In accordance with the school's requirements to have a DPO, the DPO is responsible for:

- Informing and advising the school and its employees about their obligations to comply with the GDPR in relation to photographs and videos at school.
- Monitoring the school's compliance with the GDPR in regards to processing photographs and videos.
- Advising on data protection impact assessments in relation to photographs and videos at school
- Conducting internal audits, in regards to the school's procedures for obtaining, processing and using photographs and videos.
- Providing the required training to staff members, in relation to how the GDPR impacts photographs and videos at school.

2. Parental consent

The school understands that consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

Where consent is given, a record will be kept documenting how and when consent was given and last updated.

The school ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data will be found, or the processing will cease.

Where a child is under the age of 16, the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

All parents will be asked to complete the Consent Form, which will determine whether or not they allow their child to participate in photographs and videos.

Consent will be valid unless changed in writing by the parent. With respect to media photographs, such as printed marketing material and the school website, this may extend past the child leaving Stepping Stones School.

If there is a disagreement over consent, or if a parent does not respond to a consent request, it will be treated as if consent has not been given, and photographs and videos will not be taken or published of the pupil whose parents have not consented.

All parents are entitled to withdraw or change their consent at any time during the school year but must do so in writing.

For any LAC pupils, or pupils who are adopted, the DSL will liaise with the pupil's social worker, carers or adoptive parents to establish where consent should be sought. Consideration will be given as to whether identification of an LAC pupil, or pupils who are adopted, would risk their security in any way.

Consideration will also be given to any pupils for whom child protection concerns have been raised. Should the DSL believe that taking photographs and videos of any pupils would put their security at further risk, greater care will be taken towards protecting their identity.

A list of all the names of pupils for whom consent was not given will be created by the School Office and will be circulated to all staff members. This list will be updated as and when there are changes. Staff can also check pupil consent via SIMS

If any parent withdraws or changes their consent, or the DSL reports any changes to a pupil's security risk, or there are any other changes to consent, the list will also be updated and re-circulated.

3. General procedures

Photographs and videos of pupils will be carefully planned before any activity.

Where photographs and videos will involve LAC pupils, adopted pupils, or pupils for whom there are security concerns, the Headteacher will determine the steps involved.

When organising photography and videos of pupils, the Headteacher, as well as any other staff members involved, will consider the following:

Can general shots of classrooms or group activities, rather than individual shots of pupils, be used to fulfil the same purpose?

Could the camera angle be amended in any way to avoid pupils being identified?

Will pupils be suitably dressed to be photographed and videoed?

Will pupils of different ethnic backgrounds and abilities be included within the photographs or videos to support diversity?

Would it be appropriate to edit the photos or videos in any way? E.g. to remove logos which may identify pupils?

Are the photographs and videos of the pupils completely necessary, or could alternative methods be used for the same purpose? E.g. could an article be illustrated by pupils' work rather than images or videos of the pupils themselves?

The list of all pupils of whom photographs and videos must not be taken will be checked prior to the activity.

Only pupils for whom consent has been given will be able to participate.

The staff members involved will liaise with the Deputy Headteacher if any LAC pupil, adopted pupil, or a pupil for whom there are security concerns is involved.

School equipment will be used to take photographs and videos of pupils.

Staff will ensure that all pupils are suitably dressed before taking any photographs or videos.

Where possible, staff will avoid identifying pupils. If names are required, only first names will be used.

The school will not use images or footage of any pupil who is subject to a court order.

Photos and videos that may cause any distress, upset or embarrassment will not be used.

Any concern relating to inappropriate or intrusive photography or publication of content is to be reported to the DPO.

4. Additional safeguarding procedures

The school understands that certain circumstances may put a pupil's security at greater risk and, thus, may mean extra precautions are required to protect their identity.

The DSL will, in known cases of a pupil who is an LAC or who has been adopted, liaise with the pupil's social worker, carers or adoptive parents to assess the needs and risks associated with the pupil.

Any measures required will be determined between the DSL, social worker, carers, DPO and adoptive parents with a view to minimise any impact on the pupil's day-to-day life. The measures implemented will be one of the following:

- Photos and videos can be taken as per usual school procedures
- Photos and videos can be taken within school for educational purposes and official school use, e.g. on registers, but cannot be published online or in external media
- No photos or videos can be taken at any time, for any purposes

Any outcomes will be communicated to all staff members via a staff meeting and the list outlining which pupils are not to be involved in any videos or photographs, held in the school office, will be updated accordingly. This is also recorded on pupil records on SIMS.

5. School-owned devices

Staff are encouraged to take photos and videos of pupils using school IT equipment eg school Ipads; however, they may use other equipment, such as school-owned mobile devices, where the DPO has been consulted and consent has been sought from the Headteacher prior to the activity.

Where school-owned devices are used, images and videos will be provided to the school at the earliest opportunity, and removed from any other devices.

Staff will not use their personal mobile phones, or any other personal device, to take images and videos of pupils.

Photographs and videos taken by staff members on school visits may be used for educational purposes, e.g. on displays or to illustrate the work of the school, where consent has been obtained.

Digital photographs and videos held on the school's drive are accessible to staff only. Photographs and videos are stored in labelled files, annotated with the date, and are only identifiable by year group/class number – no names are associated with images and videos.

Folders on network drives containing photographs and videos are to be deleted as soon as the class/child leaves the school. This is the responsibility of class teams and a record is to be made on the T Drive – GDPR folder – Disposal of Data Log.

6. Use of a professional photographer

If the school decides to use a professional photographer for official school photos and school events, the Headteacher will:

Provide a clear brief for the photographer about what is considered appropriate, in terms of both content and behaviour.

Issue the photographer with identification, which must be worn at all times.

Let pupils and parents know that a photographer will be in attendance at an event and ensure they have previously provided consent to both the taking and publication of videos or photographs.

Not allow unsupervised access to pupils or one-to-one photo sessions at events.

Communicate to the photographer that the material may only be used for the school's own purposes and that permission has not been given to use the photographs for any other purpose.

Ensure that the photographer will comply with the requirements set out in GDPR.

Ensure that if another individual, such as a parent or governor, is nominated to be the photographer, they are clear that the images or videos are not used for any other anything other than the purpose indicated by the school.

7. Permissible photography and videos during school events

If the Headteacher permits parents to take photographs or videos during a school event, parents will:

Remain seated while taking photographs or videos during concerts, performances and other events.

Minimise the use of flash photography during performances.

In the case of all school events, make the focus of any photographs or videos their own children.

Avoid disturbing others in the audience or distracting pupils when taking photographs or recording video.

Ensure that any images and recordings taken at school events are exclusively for personal use and are not uploaded to the internet, posted on social networking sites or openly shared in other ways.

Refrain from taking further photographs and/or videos if and when requested to do so by staff.

8. Storage and retention

Images obtained by the school will not be kept for longer than necessary.

Hard copies of photos and video recordings held by the school will be annotated with the date on which they were taken and will be stored securely. They will not be used other than for their original purpose, unless permission is sought from the Headteacher and parents of the pupils involved and the DPO has been consulted.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

Parents must inform the school in writing where they wish to withdraw or change their consent. If they do so, school will attempt to remove any related imagery and videos involving their children.

When a parent withdraws consent, it will not affect the use of any images or videos for which consent had already been obtained. Withdrawal of consent will only affect further processing.

Where a pupil's security risk has changed, if required, any related imagery and videos involving the pupil will be removed from the school drive immediately. Hard copies will be removed by returning to their parents or by shredding, as appropriate.

Official school photos are held on SIMS alongside other personal information, and are retained for the length of the pupil's attendance at the school, or longer, if necessary, e.g. due to a police investigation.

Some educational records relating to former pupils of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.