The School Photography Company
General Data Protection Regulation Policy

Introduction

The School Photography Company needs to collect and use certain types of information about the individuals and service users who come into contact with our company in order to carry out our work. This includes customers, suppliers, clients, employees and the names of school children when the school requests that we either produce data matched images on CD or group photographs with names.

This policy details how all this data, whether on paper or digital, must be gathered, handled and stored to meet the required data protection standards to adhere to the General Data Protection Regulation 2018.

The School Photography Company is Data Protection registered with the Information Commissioners Office (ICO); registration number **Z1206682**.

Data Protection Risks

This policy is aimed to protect *The School Photography Company*, individuals and service users from data security risks, which can include:

- Breaches of confidentiality.
- Failing to offer choice.
- Reputational damage.

If there is an incident of a data breach where it is deemed there is a risk then the ICO will be notified, if the breach is regarded as high risk to the rights and freedoms of individuals then the individuals concerned will be notified.

Employee Responsibilities & Rules

All employees of *The School Photography Company* have received GDPR training, to ensure they understand their responsibilities when handling data and how to review, update and/or delete any out-of-date information. Keeping data secure is a part of this training and employees are shown how to do this by using the guidelines detailed in this policy. The only staff that are allowed access to the data covered by this policy are those who need to do so to complete their job. This data should never be shared informally and the gathering and handling of personal data must be processed in line with this policy and the General Data Protection Regulation.

The key areas of responsibility are covered by:

- **The Board of Directors** are ultimately responsible for ensuring that *The School Photography Company* meets its legal obligations.
- **The Data Protection Officer**, Rhiannon Frost, is responsible for:
    - Keeping the directors updated about data protection responsibilities, risks and issues.

    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from anyone covered by this policy.
    - Dealing with requests from individuals to see the data held by *The School Photography Company.*
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries from journalists or media outlets like newspapers.
    - Make a record of all breaches regardless of whether the ICO need to be notified.
    - Notify the ICO of a data breach where it is deemed that there is a risk within 72 hours of becoming aware of it.
- **The Systems and IT Manager**, Stephen Potts, is responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services the company is considering using to store or process data.
    - Completing data audits every six months of the whole company.
    - Notifying the Data Protection Officer immediately when there is any incident of a data breach is detected.

Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

- **Office and Laboratory:**
  Computers are password protected. Any printouts are shredded when no longer required by Restore Data Shred. We have a secure entry system to all of our buildings. All images are produced by our own in-house laboratory and are then packed by our own internal packing department. We have alarm control and also have a separate secure entry system to sensitive areas of the building. Our sites are secured and monitored by ADT Security, Broadsword and Kingdom Security.
- **Photographers:**
  All of our photographers are DBS checked to the enhanced level and carry their current DBS number. Data is encrypted when the photographs have been taken and are then transferred on encrypted and password protected USB's to our Lab.
- **Sales Team:**
  All of our sales team are DBS checked to the enhanced level and carry their current DBS number. School contact information is accessed remotely via our Customer Relation Management (CRM) system. This data includes the school name, address, telephone number, a contact name and email address but no other personal details are collated. This database system is password protected and can only be accessed through the CRM system, with forced monthly changes of this password for every user. The laptops and tablets used are password protected and backed up to the company server on a regular basis.

Data Controller

The individual or organisation that provides the information to *The School Photography Company* is initially the Data Controller, and this therefore assumes that by providing the data the individual or organisation have the informed consent and permissions to do so. Once *The School Photography Company* processes this data, it becomes the Data Controller, which means that it determines for what purposes the personal information is held will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold and the general purposes that this data will be used for.

Data Collection

The School Photography Company collects data on the basis that the individual or service user gives the informed consent and has the permissions to do so. Informed consent is when:

- An individual or service user clearly understands why the information is needed, who it will be shared with, and the possible consequences of them agreeing or refusing the proposed use of the data.
- And then gives their consent.

The School Photography Company will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected on paper or digitally.

When collecting data The School Photography Company will ensure that the individual or service user:

- Clearly understands why the information is needed.
- Understands what it will be used for and what the consequences are should the individual or service user decides not to give consent to processing.
- As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed.
- Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress.

Data Processing

When personal data is accessed and processed it is at the greatest risk of loss, corruption or theft. Therefore The School Photography Company will ensure that:

- When working with personal data, employees ensure the screens of their computers are always locked when left unattended.
- Personal data is not shared informally.
- We do not disclose personal data to any third parties.
- Data must be encrypted before being transferred electronically. *The School Photography Company* advises that external contacts use a transfer service which includes encryption.
- Personal data will not be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their own computers. Always accessing and updating the central copy of any data.

Data Storage

The School Photography Company collects and uses personal data to administer orders, deliver photographs and when the school requests, to produce data matched images on a CD or provide group photographs with names. We also use relevant data to anticipate and resolve queries.

We complete data audits every six months to ensure that the data being held is up-to-date, relevant and necessary. The following details our data storage rules, which apply to data that is stored digitally or on paper:

- All data will be stored securely and will only be accessible to authorised staff.
    - When not required, all paperwork or files with personal data are kept in a locked drawer or filing cabinet.
    - Digital data is protected by strong passwords that are changed regularly and never shared between employees.
    - When data is stored on removable media (like a CD or DVD), these are kept securely on our own premises when not in use.
    - Digital data is only stored on designated drives and servers.
    - Digital data is backed up frequently and these backups are tested regularly.
    - Digital data is never saved directly to mobile devices.
    - All servers and computers containing data are protected by approved security software and a firewall.
    - Digital pupil data that is required by our photographers to provide a data match CD is stored and transferred on a secure FTP site which has regular password changes and is removed after photo day.
    - We constantly review the encryption methods and levels of our digital files that are required to be transferred. We use security software to test our network for vulnerabilities.
- All data will only be stored for only as long as required and will be disposed of appropriately.
    - All paper detailing personal information must be shredded and disposed of securely when no longer required.
    - It is our responsibility to ensure that all personal company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.
    - Data is retained for 90 days on the photographer's laptop and 18 months on the company data server to assist with queries and any late orders. The data is backed up by encrypted internal data storage. Only authorised office and lab staff have access to the data.

Data Access and Accuracy

All individuals or service users who have personal data held by *The School Photography Company* have the right to:

- Ask what information we hold about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If there is a request for information held, which is known as a subject access request, this must be received by email to dataprotection@schoolphotographs.co.uk. The Data Protection Officer will always verify the identity of anyone making a subject access request before handing over any information and will aim to provide the relevant data within 28 days.

The School Photography Company will take reasonable steps to ensure that personal data is kept accurate and up-to-date by asking data subjects whether there have been any changes.

The School Photography Company will also ensure that:

- Everyone processing personal information understands that they are contractually responsible for following good data protection practice.
- Everyone processing personal information is appropriately trained to do so.
- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them.
- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated.
- If there is a request to change personal data then a series of data questions should be asked to ensure that the request is genuine.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Disclosure

There are circumstances where the law allows *The School Photography Company* to disclose data (including sensitive data) without the data subject's consent. In these circumstances, we will disclose the requested data, however, the Data Controller will ensure the request is legitimate, seeking assistance from legal advisers where necessary.

Example circumstances are:

- Carrying out a legal duty or as authorised by the Secretary of State.
- Protecting vital interests of an individual/service user or other person.
- The individual/service user has already made the information public.
- Conducting any legal proceedings, obtaining legal advice or defending any legal rights.
- Monitoring for equal opportunities purposes – i.e. race, disability or religion.
- Providing a confidential service where the individual/service user's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill individuals/service users to provide consent signatures.

The School Photography Company regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal. *The School Photography Company* intends to ensure that personal information is treated lawfully and correctly.

To this end, *The School Photography Company* will adhere to the Principles of Data Protection, as detailed in the General Data Protection Regulation 2018.

Specifically, the Principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met.

2. Shall be obtained only for one or more of the purposes specified in GDPR and shall not be processed in any manner incompatible with that purpose or those purposes.

3. Shall be adequate, relevant and not excessive in relation to those purpose(s).

4. Shall be accurate and, where necessary, kept up to date.

5. Shall not be kept for longer than is necessary.

6. Shall be processed in accordance with the rights of data subjects under GDPR.

7. Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information.

8. Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms on individuals/service users in relation to the processing of personal information.

The School Photography Company will, through appropriate management and strict application of criteria and controls:

- Observe fully all conditions regarding the fair collection and use of information.
- Meet its legal obligations to specify the purposes for which information is used.
- Collect and process appropriate information and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements.
- Ensure the quality of information used.
- Ensure the rights of people about whom information is held, can be fully exercised under GDPR. These include:
    - The right to be informed that processing is being undertaken
    - The right of access to one's personal information
    - The right to prevent processing in certain circumstances and
    - The right to correct, rectify, block or erase information
- Take appropriate technical and organisational security measures to safeguard personal information.
- Ensure that personal information is not transferred abroad without suitable safeguards.
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.
- Set out clear procedures for responding to requests for information.

Online, Orders & Payments

The School Photography Company online photograph orders website is provided by *Xanda* who are ISO 27001 accredited and externally audited for Information Security. All information that is held on

the website is stored at Tier 1 data centres which adhere to SSAE16, PCI DSS and SOC Type 2. *Xanda* follow security best practices and have documented, tested and audited processes in place to protect data held or processed on their systems.

To order online the images can only be accessed with a unique username and password. Passwords are randomly generated with letters and numbers in lower and upper case with 8 characters, this provides 218340105584896 different combinations. Our website has a SHA-256 SSL certificate provided by Starfield Secure Certificate Authority.

Online and telephone card payments are provided by Sagepay who deal with the complete process of handling the card payments. This means that The School Photography Company do not process or store any card payment information. The payment is transacted through Secure Server Software, which encrypts all of the information so that it can't be intercepted. *The School Photography Company* are PCI DSS Compliant to level 4 with an SAQ Type A-EP and C.

Order forms that are sent to The School Photography Company can only be paid for by cash or cheque, to ensure PCI DSS compliance. The physical forms are scanned and then returned with the completed order to the customer. All scans are stored for 3 months, for customer order reference and then deleted.

Orders that are sent to home addresses are not sent with any identifiable data other than the name and address of the person who placed the order.

All customers on our website are given the opportunity for a positive opt-in for offers, consent must be given and there is the option to withdraw that consent.

Providing Information

The School Photography Company aim to ensure that all individuals or service users are aware that their data is being processed, how the data is being used and if they require, how to exercise their rights. Therefore we have a privacy policy which sets out how data relating to an individual is used by the company. This is available on our website: www.schoolphotographs.co.uk/privacy-policy/

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the General Data Protection Regulation 2018.