**Adventure Photography Ltd**

**General Data Protection Regulation (25th May 2018)**

­­­**Introduction**

Adventure Photography Ltd needs to collect certain information about individuals. This can include employees, customers, business contacts, school staff and students. In fact, anyone dealing with Adventure for the day to day running of our business in providing a product or service to you.

This policy describes how we collect, store and protect personal data. By adhering to and complying with the general Data Protection Regulation Adventure protects the data held and follows good working practise. We protect the rights of staff, customers and partners, we are open and transparent about how we collect, store and protect your data. We also protect ourselves against data breach.

**General Data Protection Regulation**

The general data protection regulation takes effect on May 25th 2018 and organisations like ours must be compliant. As Adventure already had its own data protection policy this is a small step for our business. Your data is safe with us. We safeguard it and we do not mis-use it. These rules apply no matter how and what data is stored irrespective of how long it is stored. To comply with the law , information must be collected, stored and used fairly and safely and must not be disclosed unlawfully.

Data should be collected for a specified legitimate purpose and limited to a use which is compatible with the purpose for which it is collected. Data must be accurate and where possible kept up to date. Where data is not accurate or up to date, or is no longer needed for the purpose it was collected it must be rectified or deleted securely. Data must be protected from unauthorised access, loss or unlawful processing.

**Risks and Responsibilities**

This policy applies to the staff, contractors, suppliers and any person working with or on behalf of Adventure Photography Ltd. This policy applies to all the data collected or held for Adventure photography ltd for the purpose of running the business and supplying products and services. This can include names, addresses, telephone numbers, barcodes, images and encrypted data supplied to and by Adventure Photography Ltd (this list is not exhaustive). This policy helps to protect Adventure Photography Ltd from data security risks, such as hackers, malicious software, individual data access from non-authorised personnel (this list is not exhaustive).

It is the responsibility of all staff, suppliers, contractors and working partners to inform Adventure of any breach of the contents of this policy. It is the responsibility of the Director to review this policy in line with an agreed schedule and arrange any data protection training. It is the responsibility of the office manager to inform the Director of any questions from customers relating to this policy.

**General Guidelines for data users and staff**

1. Only authorised access to those who need to use data in the course of doing their work.
2. Data should not be shared informally other than for the purpose which it is collected and saved.
3. Adventure will supply any required training for data use, protection and storage and a record of the training will be held.
4. Employees and contractors should keep data secure and take all reasonable precautions to protect data. This includes the use of passwords on all computers, servers and network devices. Passwords should only be shared with staff if it is a requirement of carrying out their contracted duties.
5. Data should be regularly reviewed and updated and if it is found to be out of date or not accurate, It should be deleted when it has no further use for the purpose it was gathered.
6. Staff should request guidance from the Director if they are unsure or unclear about any of this data policy.

**Storage of data**

Adventure may collect and use data for the day to day running of the business. This may be collected on paper or electronically. Electronic data may have to be printed out.

All paper date must be stored safely and locked away when not in use or out of business hours. Once papers copies are no longer required these should be returned to the customer or securely destroyed. This is done by cross cut secure shredding or incineration.

When data is stored electronically this should be encrypted, anonymised or password protected. Passwords should not be shared amongst unauthorised personnel and should only be shared if it is a requirement of the production process.

If data is stored on removable media it should be kept in a locked cabinet when not in use. Data should only be stored on designated devices supplied by Adventure Photography Ltd.

Data is backed up regularly and these are also securely deleted once they are no longer required.

All servers and computers are protected by security and firewall.

All pupil information supplied by schools for linking images to the school database should be provided by the school as a password protected file. This is encrypted once received by Adventure. Photographers who are enhanced DBS checked are then supplied barcodes in paper form. These are returned to Adventure office immediately after the photo shoot and securely destroyed. This information can only be accessed by staff authorised to do so in order to carry out their contracted duties.

**Supplier agreement and access to data**

The suppliers of Adventure digital workflow software solution may from time to time have to carry out system integration, upgrades and maintenance. This may be done remotely via a point to point secure connection. This supplier has entered into a non-data sharing agreement with Adventure and only nominated employees have access privileges. Adventure has also entered into a no-share agreement with the supplier for additional security. This agreement is updated and reviewed annually.

**Office administration staff**

Adventure office administration staff, including production staff have limited authorised access to data and will only be able to access data in order to carry out their contracted duties. Authorised staff have access to passwords for their work station on a local basis and are not privy to other passwords used on our internal network. A firewall is in place to protect the internal network from external unauthorised access.

 Data held on our internal server is password protected and only the Director and Senior Production Manager have additional clearance to passwords. No single staff member will have access to all the passwords.

**Our photographers**

All Adventure Photographers are enhanced DBS checked and carry photo I.D. with them when working alongside children and young adults in schools, nurseries, playgroups and clubs. Adventure photographers also wear clothing branded with the company logo whilst working. Adventure have a code of conduct which our photographers must adhere to at all times. Adventure photographers will also adhere to your setting phone policy whilst working with you.

**Our professional photo lab**

Adventure use a professional photo lab which trades under the name of CC Imaging Photo lab Ltd. It is wholly owned by the director of Adventure Photography Ltd and is situated in the same premises as Adventure. It is the Adventure service provider for printing. We do not outsource our manufacturing process. Adventure staff pack and manufacture within our premises all the other products we supply. Waste prints are shredded securely or incinerated.

**Our security**

Adventure premises are secure with a gated electrically operated password protected entry outside normal working hours. Adventure offices are protected with a secure and 24hr monitored system. The building is also secured with additional measures such as barred windows and security shutter protection to windows and access points. We also have additional password protected gates around the premises with on-site security surveillance.

**Servers**

Adventure temporarily store images on our internal secure server. These are deleted once they are no longer required. This process is reviewed every six months. We do not store hi resolution images in the cloud. We do upload encrypted low resolution images to our web shop for your viewing. These are also watermarked.

**Payments**

Adventure online orders have an encrypted system which can only be accessed by the customer through a unique random 8 digit reference which is a combination of 24 letters and 10 numbers used in conjunction with a password. Our chosen payment partner is PAYPAL and you will be redirected to their secure payment portal. Adventure have no access to this. Should you not wish to use our online system you can choose to pay using a card. Our chosen payment partner for this is Barclays and we are fully PCI compliant and adhere to the information security policy document supplied by Barclays. We do not have access to payment data other than that supplied by you required to process the one off transaction for your purchase. This information is not stored. Any paper orders collected from your school will always be collected by one of Adventure staff. An Adventure collection note will require a signature and our staff carry photo ID. We do not use external companies or individuals to collect orders from schools.

Document prepared by Chris Rose

Review date 24.05.2019