

David Hughes Photography & Video and Phototheme

David Hughes is a Sole Trader trading as:
David Hughes Photography & Video
and
Phototheme

DHP&V and Phototheme

Data Protection and ICO Registration

Data Protection

Data protection is about ensuring information is collected and stored appropriately. Protecting data is a legislative requirement under the Data Protection Act 1998 and the General Data Protection Regulation (GDPR) laws that came into effect on 25th May 2018.

David Hughes Photography & Video and Phototheme comply with these acts and regulations and our data.

David Hughes is a Sole Trader trading as:
David Hughes Photography and Video
and
Phototheme

David Hughes Photography & Video fully complies with all aspects of the data protection act.

We hold no personal data on any individual other than the contact details of those people who engage our photographic and video services and the date and location of that event on our booking forms.

We have email addresses of clients within our contacts on our email program but that data is never shared.

That information is kept on a password protected computer.

Our Incoming email is stored on Silkwebs', (our Domain hosting company) secured servers and when received remains there until downloaded by us.

Outgoing email is authenticated (to show it is genuine) by their servers, but then simply sent and not stored. We and our provider use industry standard SSL/TLS security for both our incoming and outgoing mail.

We don't do any e-commerce through our websites although they are secure, but have two different companies that provide online ordering for us (and others) and is also secure.

The names of brides and grooms and venues of weddings on finished videos and photographic images are essential parts of the finished media and all images and video are kept on password protected external RAID 1 HDDs.

We rent a first floor office within a Havering Council building and our office has only one entry point which is secured by a BS3621 5 lever deadlock as specified by our insurers.

Within the building there is CCTV which monitors access to our office and other areas of the building and grounds and is displayed and recorded in the building reception. That monitoring gives added security during the day and at night the building is alarmed with a sensor in our office and the alarm system is centrally monitored.

We process thousands of images of objects and people through our general photography business and tens of thousands of images of children each year through our school and preschool photography business.

Much of our school business is conducted online.

Online ordering is handled by our dedicated school photography laboratory and access by parents to the ordering process is via a unique 13 digit reference number on the paper proof sheet containing their child's images.

Orders through the school are made on our paper proof sheets and we only accept cash or cheque and occasionally bank transfer.

The finished prints are returned directly to the school or the parents' homes by our lab and the proof sheets shredded and recycled.

Our Phototheme website has many images of children all of which have written consent from parents and we keep the consent forms locked in our office.

When we do use images on our website or our Facebook page we never identify the school or preschool at which that the image was taken and never include names.

Generally our policy regarding images includes the following.

We do not use children's names in photograph captions.

We ALWAYS use a parental permission form to obtain consent for use of an image of a child.

Depending on the child's age we may also ask for permission from them.

When photographing in schools and preschools we INSIST, as should be their

safeguarding policy and to safeguard us, that we are never left alone with children.

Our data protection policy is copied below

David Hughes Photography & Video and Phototheme
19 Waycross Road
Cranham
Upminster
Essex
RM14 1LZ

What is the GDPR?

GDPR is the General Data Protection Regulation laws that come into effect on 25th May 2018, the law is to ensure that business are compliant and have strict practices in place for managing and handling peoples' data. David Hughes Photography & Video and Phototheme has conducted a full audit of our working practices which will be ongoing and reviewed regularly. This includes collection, handling, ocumentation, processing, storage and deletion procedures.

Context and overview

Key details:

- Policy prepared by: David Hughes
- Policy became operational on: 25/05/2018

Introduction

David Hughes Photography & Video and Phototheme needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards - and to comply with the law.

Why this policy exists

This data protection policy ensures David Hughes Photography & Video and Phototheme

- Complies with data protection law and follow good practice
- Protects the rights of staff, customers and partners

- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The Data Protection Act 1998 describes how organisations - David Hughes Photography & Video and Phototheme - must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully.
2. Be obtained only for specific, lawful purposes.
3. Be adequate, relevant and not excessive.
4. Be accurate and kept up to date.
5. Not be held for any longer than necessary.
6. Processed in accordance with the rights of data subjects.
7. Be protected in appropriate ways.
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

People, risks and responsibilities

Policy scope

This policy applies to:

- The head office of David Hughes Photography & Video and Phototheme
- All branches of David Hughes Photography & Video and Phototheme
- All staff and volunteers of David Hughes Photography & Video and Phototheme
- All contractors, suppliers and other people working on behalf of David Hughes Photography & Video and Phototheme
- It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals

- Postal addresses
- Email addresses
- Telephone numbers
- ...plus any other information relating to individuals

Data protection risks

- This policy helps to protect David Hughes Photography & Video and Phototheme from some very real data security risks, including
- Breaches of confidentiality. For instance, information being given out inappropriately
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data

Responsibilities

Everyone who works for or with David Hughes Photography & Video and Phototheme has some responsibility for ensuring data is collected, stored and handled appropriately. Each person that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. However, these people have key areas of responsibility:

- Arranging data protection training and advice for the people covered by this policy
- Handling data protection questions from staff and anyone else covered by this policy
 - Dealing with requests from individuals to see the data David Hughes Photography & Video and Phototheme holds about them (also called 'subject access requests')
 - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data

David Hughes 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. For instance, cloud computing services

David Hughes is responsible for:

- 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

Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General staff guidelines

- The only people able to access data covered by this policy should be those who need it for their work
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers
- David Hughes Photography & Video and Phototheme will provide training to all employees to help them understand their responsibilities when handling data

- Employees should keep all data secure, by taking sensible precautions and following the guidelines below
- In particular, strong passwords must be used and they should never be shared
- Personal data should not be disclosed to unauthorised people, either within the company or externally
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to David Hughes. When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet
- Employees should make sure paper and printouts are not left where unauthorised people could see them

- Data printouts should be shredded and disposed of securely when no longer required
- When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts
- Data should be protected by strong passwords that are changed regularly and never shared between employees
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services
- Servers containing personal data should be sited in a secure location, away from general office space
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones
- All servers and computers containing data should be protected by approved security software and a firewall

Data use

Personal data is of no value to Phototheme unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure
- Data must be encrypted before being transferred electronically
- Personal data should never be transferred outside of the European Economic Area
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data

Data accuracy

The law requires Phototheme to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Phototheme should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- 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, for instance, by confirming a customer's details when they call
- Phototheme will make it easy for data subjects to update the information Phototheme holds about them
- 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

Subject access requests

All individuals who are the subject of personal data held by Phototheme are entitled to:

- Ask what information the company holds 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 an individual contacts the company requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to David Hughes, email address, info@photothem.co.uk. or info@dhpgotography.co.uk. We can supply a standard request form, although individuals do not have to use this. Individuals will be charged £10 per subject access request. We will aim to provide the relevant data within 14 days. We will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, Phototheme will disclose requested data. However, we

will ensure the request is legitimate, seeking assistance from our legal advisers where necessary.

Providing information

David Hughes Photography & Video and Phototheme aims to ensure that individuals are aware that their data is being processed and that they understand:

- How the data is being used
- How to exercise their rights

END