LITTLEHAMPTON & DISTRICT CAMERA CLUB

Friendly photography

DATA PROTECTION POLICY

1 OVERVIEW OF THE GENERAL DATA PROTECTION REGULATIONS (GDPR)

The General Data Protection Regulations are a legal framework which came into effect on 25 May 2018 and which sets guidelines for the collection and processing of personal data of individuals.

The main principles of the GDPR requires that any personal data held should:

1. be fairly and lawfully processed
2. be obtained and processed for limited purposes and not in any manner incompatible with those purposes
3. be adequate, relevant and not excessive
4. be accurate and kept up to date
5. not be kept for longer than is necessary
6. be processed in accordance with individuals' rights
7. be secure with appropriate technical and organizational measures taken to prevent unauthorized or unlawful processing of personal data and against accidental loss or destruction or damage to personal data; and
8. not be transferred to countries without adequate protection

GDPR also gives individuals certain rights as follows:

1. The right to be informed if their personal data is being collected and used
2. The right of access gives individuals the right to obtain a copy of their personal data as well as other supplementary information which largely corresponds to the information that should be provided in a privacy notice
3. The right to rectification if the personal data held is inaccurate or incomplete
4. The right to erasure is also known as the right to be forgotten and is applicable in certain specific circumstances.
5. The right to restrict processing allows individuals to limit the way that an organisation uses their data in certain circumstances and can be used as an alternative to requesting the erasure of their data.
6. The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services but is only applicable if the organisation's lawful basis for processing this information is consent **or** for the performance of a contract; and the processing is being carried out by automated means (ie excluding paper files).
7. The right to object gives individuals the right to object to the processing of their personal data, which effectively allows individuals to ask an organisation to stop processing their personal data in certain circumstances.
8. Rights in relation to automated decision making and profiling where there is no human involvement in the decision making.

The key definitions under GDPR are:

1. Personal data
2. Controller
3. Processor

1. Personal Data: this is any information that can be used to directly or indirectly identify a particular individual. The information, such as name, identification number, postal address, email address, maybe held electronically or on paper. Personal data that has been pseudonymised – e.g., key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual. Personal data may also include any expression of opinion about an identifiable person or any indication of the intentions of the Controller or any other person in respect of the individual.

   Some types of personal data are defined as "*Special Category Data*". Such information includes racial or ethnic origin, religious beliefs, political affiliation, trade union membership, genetics, biometrics, health and, sexuality, commission or alleged commission of any offence and any related proceedings. Additional protection needs to be incorporated into processes used for handling Special Category Data since such data could create more significant risks to a person's fundamental rights and freedoms - e.g., by putting them at risk of unlawful discrimination.

2. Controller: a controller determines the purposes and means of processing personal data. Controllers are also obliged to ensure that their contracts with processors comply with The GDPR.

3. Processor: a processor is responsible for processing personal data on behalf of a controller. The GDPR places specific legal obligations on Processors; e.g., they are required to maintain records of personal data and processing activities. Processors will also have legal liability if they are responsible for a data breach.

2 DATA PROTECTION POLICY

In the course of your tenure as a Committee Officer, Committee Member, Non-Committee Post Holder or Co-opted Member, you may come into contact with and use personal information about Club members, such as names, postal addresses, telephone numbers and email addresses.

Although Littlehampton & District Camera Club (LDCC) is exempt from registration with the Information Commissioners Office, we are still required to comply with the GDPR.

This policy describes how personal information is collected, handled and secured to ensure that our processes do not breach the legal framework of the GDPR. If you are in any doubt about what you may or may not do seek advice from the Committee Officers.

A separate document called the LDCC Privacy Notice contains the following information:

- Who we are
- Details of personal information that we collect from and about Members
- How we use personal information belonging to Members
- Our legal basis for processing personal information belonging Members

- Who we might share the personal information with
- The rights of individuals about whom we hold personal information
- Our data retention policy
- How we can be contacted

Individuals about whom we hold information are referred to in this policy as Data Subjects.

This policy applies to all Committee Officers, Committee Members, Non-Committee Post Holders or Co-opted Members, as well as the LDCC Accounts Examiner and any other organisations, service providers and specialist advisers that may be used by LDCC.

Collecting and Holding of Personal Information

- We maintain accurate information and have procedures in place so that Data Subjects can update the information held about them via requests to the Club Secretary.
- We do not hold information about individuals without their knowledge and consent. It is a legal requirement that people know what we are doing with their information and who it will be shared with.
- We only hold information for specific purposes. We will inform Data Subjects what those purposes are. We will also inform them if those purposes change.
- Special Category Data as defined under the GDPR is not required by LDCC to conduct its business. Any proposed holding of sensitive personal information by LDCC needs to be reviewed and agreed by the Committee and will also require the Data Subject's specific consent.

Access to Information

- Information about Data Subjects will not be disclosed to other organisations or to individuals who are not covered by this Policy except in circumstances where this is a legal requirement, where there is explicit or implied consent, or where information is publicly available elsewhere. Committee approval is required for any deviation from this rule and the affected individual or individuals need to be informed prior to the information being shared.
- Data Subjects are entitled to have access to information held about them by us and for what purpose. We refer to this as Subject Access. We will act on the subject access request without undue delay and at the latest within one month of receipt of the request.
- In most cases we will not charge a fee to comply with a subject access request. However, if we believe that the request is manifestly unfounded or excessive we may charge a "reasonable fee" for the administrative costs of complying with the request. We may also charge a reasonable fee if a Data Subject requests further copies of their data following a request. We will base the fee on the administrative costs of providing further copies.
- At the beginning of a new project or type of activity the individual managing it will consult the Committee about any data protection implications.
- Data Subjects can opt not to receive mailings from us which are not strictly necessary to conduct the business of LDCC.

Data Security

- Any personal information held electronically will be stored on computers that are password protected.
- Any personal information held as paper records will be kept in locked premises, usually the home of the owner.
- Any personal information (such as postal address or contact number) but excluding a Data Subject's name, will not be sent in the body of an email. If such information has to be shared via email then it must be sent as a password protected file. Such emails should be deleted as soon as they are no longer required.
- If an email needs to be sent to multiple Members, their Emails Addresses MUST ONLY be added to the BCC field.
- All passwords MUST be at least 8 characters long and contain upper and lower case letters, a number and ideally a symbol. This will help to keep our information secure. There is no point protecting the personal information we hold with a password if that password is easy to guess.
- All portable devices – such as memory sticks and laptops – when not being used at a Club Meeting will be kept in locked premises, usually the home of the owner.
- All computers holding LDCC data should be protected by approved security software and a firewall.

Data Breaches

- In the event of a personal data breach, the LDCC Club Secretary will, without undue delay and where feasible, not later than 72 hours of becoming aware of the breach, notify the Information Commissioner's Office (ICO) unless LDCC is able to demonstrate that the breach is unlikely to result in a risk to the rights and freedoms of individuals.
- Where the above aim cannot be achieved within 72 hours, an explanation of the reasons for delay will accompany the notification to the ICO and information may be provided in phases without undue further delay.
- In addition, data subjects will be notified without undue delay if the personal data breach is likely to result in a high risk to their rights and freedoms to allow them to take the necessary precautions. This notification will describe the nature of the personal data breach as well as recommendations for the individual concerned to mitigate potential adverse effects. This will be done as soon as reasonably feasible, and in close co-operation with the ICO.

Our Commitment

- All new Committee Officers, Committee Members, Non-Committee Post Holders or Co-opted Members will be asked to review this Data Protection Policy and given training on how they should store and handle personal information.
- We will review our data protection policy and procedures every two years. This version of the policy was most recently updated on 11 September 2020.