Data Protection Principles

The Institute of Quarrying

Data protection refers to how personal information is used by organisations, businesses and government. It is controlled through the Data Protection Act (1998), which sets out the basic principles that people with access to data must follow. The main aim of the Act is to protect individuals from misuse or abuse as a result of the information held about them.

What is it?

The Data Protection Act sets out what information is affected, the circumstances in which data is protected and the roles and responsibilities of people involved.

The principles of the regulations can be summarised as:

Personal data should be processed fairly and lawfully and only obtained for one or more specified and lawful purpose(s), it shouldn't be further processed for any other reason	You must have legitimate grounds for collecting data and use it how you would reasonably expect. Be clear why you collect information and what you need it for.
Personal data should be adequate, relevant and not excessive in relation to the purpose(s) it is being processed for	Collect only the minimum amount of data you need. You should not hold personal data on the off-chance that it might be useful in the future.
Personal data should be accurate and, where necessary, kept up to date	It's okay to keep records of events that happened providing these records are accurate.
Personal data processed for any purpose(s) should not be kept for longer than absolutely necessary	There is no maximum time you can keep records, the Act only states that personal data shall not be kept for longer than is necessary. Do not hoard data on the off chance it may be needed in the future.
Personal data should be kept safe, secure and not be transferred outside the European Economic Area, unless that country has adequate protection in place	Do you use cloud storage such as OneDrive, Dropbox or Google? These often store data in the US so you would be transferring data outside of the EEA. These market leaders meet the rules on data storage but other service providers may not.
Personal data should be processed in accordance with the rights of data subjects under the Data Protection Act	Protection rights include data not being used for marketing, unless they have opted in to receive this.

In line with these principles and to help branches communicate effectively at a local level, a centralised emailing system to notify members of activities and events has been created.

This is the only emailing system to be used for notifying branch members of such activities. Individual volunteers should not use their personal or work emails to send these communications.

General branch notifications should still be sent out from head office in the usual way, but should an event cancellation or last minute change to a planned event need to be communicated to members during out of office hours, each branch will have their own access to this account to facilitate this.

To access this system please refer to the user guidance and login details provided to the branch Chairman and Secretary.

Why is it important to me?

Data Protection is a crucial part of the activities of the Institute of Quarrying and everyone in the Institute including staff, volunteers and members have a duty to follow the principles of data protection.

As a responsible organisation, the principles of data protection will apply to all of the Institute's policies and procedures.

Where Next?

Further detailed information is available in the IQ Branch Data Protection Guidance, which has been issued to all branch Chairman and Secretaries.

If you have any queries or would like to raise any concerns please contact us on 0115 972 9995 or mail@quarrying.org.