

CCTV POLICY

CCTV is used at Lincombe Boatyard. It is managed in line with the Data Protection Act and other legislation. The controller is Winters Marine Ltd which has registration at the ICO (Information Commissioner's Office).

This policy applies to employees, officers, consultants, tenants, contractors, casual workers, agency workers, volunteers, and interns. It also applies to anyone visiting the premises.

Cameras are located at various points throughout the premises, including entrance/exit points and moorings. Signs are visible in various locations to inform that CCTV is in operation.

Cameras record 24 hours a day, 7 days a week. Recordings are overwritten on a regular basis once the storage capacity has been reached. Once overwritten the images are permanently deleted. If an investigation is ongoing this period of time may be extended.

CCTV is used for the following purposes, which Winters Marine Ltd believes is necessary for business purposes:

- Monitoring of site and public areas
- Detection and prevention of crime
- Identification for prosecution
- Security of the business premises
- Procedures and H & S rules are being followed.
- Identification of unauthorised activity, unsafe working, and malpractice to assist with evidence gathering.

The above is a summary and not exhaustive.

Access and disclosure of images is restricted to the controller and any persons who have a legitimate reason to access or review footage, this ensures that individuals rights are maintained.

Images can only be disclosed in accordance with the purposes for which they were originally collected, this includes to third parties who will be limited to

- The police and law enforcement agencies where the images would assist with detection and prevention of crime, or the identification and prosecution of an offender or identify a victim or witness.
- Prosecution agencies i.e. Crown prosecution service
- Legal representatives with a relevant need.
- Managers involved with the controlling of company disciplinary procedures.
- Individual's images unless disclosure would prejudice the prevention or detection of crime or the arrest/prosecution of an offender.

The controller is the only one who is permitted to authorise the disclosure of images to third parties.

Requests for disclosure and access to images will be documented with a date, reason and if access denied the reason why.

UK Data Protection laws, including GDPR (General Data Protection Regulation) ensures data subjects have the right, on request, to view the personal data that a company holds about them, including CCTV if they are recognisable.

If you wish to access any images relating to you, a written request must be made to the controller in line with requests from third parties.

A charge will not normally be made for any requests, but the controller reserves the right to charge if the request is unfounded, excessive, or repetitive.

Any request must include the date, location, and time.

A response will be given within one month; however, complex, and large requests may take longer.

Identity checks may be needed before carrying out a data subject request. If third parties need to be obscured from requested images to protect their privacy, and this is not possible, then access may be refused.

If it has not been possible to comply with a request because it could prejudice the prevention or detection of crime, or the arrest or prosecution of an offender, this will be advised at the time.

It may be necessary to conduct covert recording, this will be done in exceptional circumstances where reasonable grounds suggest that criminal activity, or serious malpractice is taking place, and there is no other less intrusive way to do this.

A data protection impact assessment will be undertaken prior to any covert recording. This will consider the purpose, need, risks to privacy of individuals, time limits and compliance with data protection and GDPR.

If after undertaking a data impact assessment it is deemed necessary, due to a risk of informing the individuals concerned would affect the prevention or detection of crime, then the company will covertly record the suspected individual for a reasonable and limited amount of time.

The company will rely on the protection of its own interests as the lawful and justified reason. Covert recording may include video and audio. The same access to all recordings will apply.

The policy will be reviewed periodically to ensure surveillance remains necessary and appropriate.