DATA PRIVACY & PROTECTION POLICY

CONTENTS

1. DATA PROTECTION IN OSC 1
2. RIGHT TO COMPLAIN 3
3. CONTACT INFORMATION 3

LIST OF ACRONYMS/ABBREVIATIONS/UNITS/TERMS

CCTV	Closed-Circuit TeleVision
DPA	Data Protection Act 2018
GDPR	General Data Protection Regulation
ICO	Information Commissioners Office
IT	Information Technology
OSC	Ocean Science Consulting Limited

1. DATA PROTECTION IN OSC

OSC is committed fully to abiding by the relevant data protection laws such as the Data Protection Act (DPA) 2018, and General Data Protection Regulation (GDPR) (EU) 2016/689. To this effect, OSC will obtain, handle, process, store, and destroy personal information, as required under DPA and GDPR.

What data does OSC collect?

- Closed-Circuit TeleVision (CCTV) system operates 24/7 (around/inside any OSC premises, including and not limited to workshops, offices, warehouse, and vessels, for the purpose of keeping employees safe, and secure, to prevent crime, to prevent employee misconduct, and for the health and safety of employees);
- Personnel biometric forms (for the purpose of offshore work);
- Personnel documents (including and not limited to passports, driving licences, medical certificates for the purposes of offshore work);
- Personal contact information (including and not limited to email, phone number, and address); and,
- The Company monitors and records telephone calls, electronic communications and information viewed or transmitted on computers and networks used for Company business. If you choose to use email, the internet or make telephone calls for personal purposes you should not expect privacy.

OSC is committed to:

- Ensuring we comply with the seven data protection principles;
- Meeting our legal obligations as laid down by DPA and GDPR;
- Processing personal data only in order to meet our operational needs or fulfil legal requirements;
- Ensuring all staff have read and understood this policy document;
- Providing adequate training for all staff responsible for personal data;
- Only providing personal data to outside companies if necessary for your legitimate interest, with explicit consent, and, or it is necessary for the performance of a contract;
- Ensuring anyone handling personal data knows where to find further guidance;
- Ensuring all staff contact the nominated Data Privacy Officer if in any doubt, and not to jeopardise individuals' rights or risk a contravention of GDPR;

- Ensuring that queries about data protection, internal and external to the organisation, are dealt with effectively and promptly; and,
- Regularly reviewing data protection procedures and guidelines within the organisation.

Following data protection principles, OSC ensures information is:

1. Used fairly and lawfully;
2. Used for limited, specifically stated purposes;
3. Used in a way that is adequate, relevant, and not excessive;
4. Accurate and, where necessary, kept up to date;
5. Kept for no longer than is absolutely necessary;
6. Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage
7. Not transferred outside the UK without adequate protection.

Who has access to data and how long is stored?

- CCTV: only top-tier management have access to encrypted hard-drives, upon pursuit individuals can request CCTV footage which has them in, OSC has two months to deliver footage. CCTV will be passed onto police if a suspected criminal incident has arisen. CCTV is clearly advertised around all OSC premises, data is only stored as long as necessary;
- Personal data: only those who require your data under GDPR principles will have access. Your data is secured through our IT system, which works under a tiered access system. OSC will only distribute data to outside parties where essential, in full compliance to GDPR; and,
- Marketing: OSC will contact personnel through appropriate channels to notify about offshore work, and discuss thereafter those who no longer wish to receive this information can opt out, and their information will be deleted or returned to individual upon request.

OSC can conduct system monitoring, which can include but is not limited to email screening, computer profile monitoring, and web history searches for the purpose of staff security and IT system security.

CCTV has been installed to ensure the safety of staff and visitors on Company property, to assist in prevention and detection of crime, to facilitate identification, apprehension, and prosecution of offenders in relation to crime on Company premises; to assist with identification of actions that may result in disciplinary proceedings between and against staff, to monitor and assist with traffic management issues on company premises, to reduce the fear of crime and to reassure staff and visitors. The CCTV system operates throughout the year for 24 hours a day. Images captured on CCTV are recorded on a secure digital hard drive and encrypted streaming. For the purposes of the General Data Protection Regulation 2016 and the Data Protection Act 2018, the Data Controller and the Company is legally responsible for management and maintenance of the CCTV system. Images captured by the system are monitored on encrypted devices, and stored in a self-contained, secure, and restricted area. Other than emergencies, no unauthorised access to the footage is allowed at any time. Normal access is limited strictly to authorised persons, including: Directors and Line Managers, management staff with remote viewing monitors, Police officers, Data Protection Officer, Other statutory officers, *e.g.* Health & Safety Executive officers, and authorised employees of contractual suppliers in place for CCTV. CCTV images may be personal data and therefore fall within the scope of the General Data Protection Regulation 2016, the Data Protection Act 2018 and all applicable privacy laws.

OSC recognises and understands the consequences of failure to comply with the requirements of DPA and GDPR.

OSC is registered under the Information Commissioners Office (ICO) to ensure GDPR compliance for CCTV.

2. RIGHT TO COMPLAIN

Should you feel that OSC is mishandling your data, you can report your concern to the ICO. For more information visit the ICO website.

3. CONTACT INFORMATION

If you have any concerns in regards to OSC GDPR practices contact our designated GDPR officer: Sophie Cox
Email: sc@osc.co.uk
Address: OSC, Spott Road, Dunbar, EH42 1RR

Action	Name	Function	Date	Signature
Audit	Dr Victoria Todd	Managing Director	09/11/2023	
Audit	Ian Todd	Managing Director	09/11/2023