

GDPR DATA POLICY STATEMENT

PURPOSE AND SCOPE

All Sub-Contractors, Employees and customers have the right to know and be informed of any personal data which is held by Creative Protection Services Ltd and be supplied with a copy if they wish.

All personal information held by Creative Protection Services Ltd is stored securely and only accessed or shared with those who are authorised.

In the case of a breach of security or data, immediate action is taken to minimise the risk, to all parties.

SCOPE & PROCEDURE

Creative Protection Services Ltd is required to:

- Obtain and process personal data fairly and lawfully.
- Hold personal data only for specified purposes.
- Use or disclose personal data only in a way which is compatible with those purposes.
- Maintain the accuracy of personal data held.
- Ensure that the personal data held is relevant and adequate.
- Maintain appropriate security measures in relation to the storage of personal data.
- Keep data for only if necessary.
- Ensure that personal data is shared only with those who have the right to it. This includes Her Majesty's Revenue and Customs, The Security Industry Authority and Training Awarding bodies
- Inform customers, staff, and sub-contractors of what data we store, why we store it, how we store it and how we share it.

ACCESS TO RECORDS

Employees, Sub Contractors and Trainees who wish to receive a copy of their personal data, either held on computer or in paper form should contact their Line Manager or the Directors of Creative Protection Services Ltd.

As such they are requested to check the accuracy of the data and inform the Directors of any amendments that need to be made.

Any customers requiring access to their records should make the request to the Directors of Creative Protection Services Ltd, in writing on headed notepaper. If the customer is an individual without headed notepaper then the data will be sent, via recorded post to the address held on file. Alternatively, a customer could arrange an appointment to visit the office to view their data.

RETENTION OF RECORDS

Records must be kept for the required length of time as per the Control of Records Policies and Procedures.

BREACHES OF SECURITY OR DATA PROTECTION

Creative Protection Services Ltd has a responsibility under the General Data Protection Regulations (GDPR) 2016 to ensure the appropriate and proportionate security of the data it holds. Although this responsibility is taken very seriously there may be occasion where there is a data security breach.

In such circumstances the following procedures will be followed:

- The Directors will be informed immediately or in their absence the Security Manager.
- The nature of the breach will be advised, example of this is this has it been lost, shared, stolen, or unlawfully obtained, what data is involved, the nature of the data and how many people it potentially affects.

The Directors will:

- Consider who needs to be made aware of the breach.
- Who is needed to assist with any further investigation?
- How the breach can be minimised and contained
- Do the police need to be informed?
- Undertake a risk assessment which takes into consideration:
 1. What type of data is involved?
 2. How sensitive is the data, eg; can it be misused (bank account details etc)
 3. Is the data protected, eg; passworded or encrypted?
 4. What has happened to the data, eg; lost or stolen
 5. What information could the data give a third party?
 6. How many individuals' personal data is affected by the breach and who are they
 7. What harm could come to those individuals?
 8. Are there any wider consequences to the loss?
- Notify the individual(s) affected.
- Consider notification to the Information Commissioners Office
- Notify any other Regulatory Bodies.
- Take remedial action to minimise the risk.
- Review policies and procedures to minimise future risk.

The Data Protection Act 1998 superseded by **GDPR** 2016; Control of Records Policy; **GDPR** Privacy Notice; **GDPR** Control Document



Revision B

Issued May 2021

Review May 2022

Form No 0034/B

This Policy will be regularly reviewed and updated, as necessary. The management team endorses these Policies and is fully committed to their implementation.

This policy has been approved & authorised by:

Name: Mr Scott Taylor **ASyl**

Position: Business Director

Date: 25th May 2021 (Expiry date 24th May 2022)

Signature: *S Taylor*