Section 1 Purpose

The purpose of this policy is to define the measures taken to ensure Security issues do not become an issue within the company.

Section 2 Scope

This document applies throughout DFP Services Limited on all contracts carrying out all services.

Section 3 Policy

It is the policy of DFP Services Limited to ensure adequate security arrangements are in place so as to protect the following: -

- DFP Worksites (Preventing Items being stolen, and trespassers being injured),
- DFP Employees and their personal belongings,
- DFP client's information,
- IT Hardware and software.

Personal property

The company will not be held accountable for personal property; however, a control system will be set in place so restricting access to visitors, contractors and clients alike. All visitors will be accompanied by a DFP employee who will act as a guide for the visitor.

Company property

Individuals are responsible for any company equipment or documents issued whilst in the company's employment.

On the termination of your employment, or at any other time in accordance with instructions given to you by the company, you will immediately return to the company all equipment, company clothing, correspondence, records, specifications, software, models, notes, reports and other documents and any copies thereof and any other property belonging to the company (including but not limited to keys, mobile phones, credit cards, keys and passes) which are in your possession or under your control.

General rules for company security

Personal effects should at no time be left unattended. The company does not accept responsibility for the loss, damage, or disappearance of personal effects. Notwithstanding this policy, any losses must be reported immediately to the company so that prompt action can be taken to attempt recovery and necessary measures can be taken to prevent a recurrence.

DFP sites must be left in a secure state at all times, a site security guard where necessary or as a minimum, Harris fencing around the site perimeter, Plant and equipment will be left behind the security fencing or returned to the nominated yard/ depot. Keys for such equipment must always be removed and when the equipment is not in use and removed from site after the working shift has been completed. The taking of materials, plant or equipment without authority will not be tolerated and any person caught doing so will be instantly dismissed. The incident will also be reported to the police.

THE COMPANY RESERVE THE RIGHT TO INSPECT AND SEARCH VEHICLES AND BAGS LEAVING DFP PREMISES.

The security of plant and equipment is an expected part of an employee's duties. Here are some good practices that must be observed. -

- Ensure vehicles are locked at all times - even when you are working close by.
- Do not leave plant, equipment and tools unattended.
- Compressors and other trailers must be secured with towing locks or chain and padlocks.
- Except in exceptional circumstances plant and equipment should be left in secure compounds.

Failure to adhere to the above minimum requirements may result in disciplinary measures being taken. Any employee found to have left a key in a vehicle whilst it is unattended will be guilty of 'Gross Misconduct'.

Section 4 Specific Requirements for the GDPR 2018

The General Data Protection Regulations come into force in May 2018, the regulations place requirements on businesses to further control and protect personal data held within the organisation.

DFP Will ensure we comply with the regulations by undertaking the following: -

1. Awareness - We will ensure that decision makers and key people in the organisation are aware that the law relating to GDPR. GDPR will be added to the Business Risk Register and reviewed as part of the management review process, and we will ensure that sufficient resource is in place to manage the requirements of GDPR.

2. Information Held – We will document the following: -
    a. What personal data we hold,
    b. Where it came from,
    c. Who we share it with.
    d. How we Audit the information held.
    e. How we process / Use the information we hold.

3. Communication of privacy information – We will inform all stakeholders of the information we hold and what we will use this information for.
    a. Why we will be using their data
    b. Our Retention Periods for keeping the data
    c. Our data disposal protocols
    d. How individuals can complain about the data we hold on them.

    DFP Services Ltd will inform all relevant parties and request if they would like to 'opt-in' (allow us to keep/ store their data).

4. Individuals' rights – We will ensure our procedures cover all the rights of individuals including: -
    a. The right to be informed of the data held
    b. The right of easy access to the data
    c. The right to rectification;
    d. The right to erasure;
    e. The right to restrict processing;
    f. The right to data portability;
    g. The right to object;

5. Subject access requests – We will grant data access requests free of charge, requested data will be provided to the individual within 28 days of the request. The company reserves the right to refuse a request, in which case we will tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy.

6. Lawful basis for processing personal data – Data held within the organisation is held so as to comply with current HR regulations, Asylum and Immigration regulations and where necessary contractual requirements. Data outside these parameters will not be held by the organisation.
7. Consent – We will seek and record consent. Consent will be freely given, specific, informed and unambiguous. There will be a positive opt-in – consent will not be inferred from silence, pre-ticked boxes or inactivity. It will also be separate from other terms and conditions, and we will have simple ways for people to withdraw consent.

8. Children – We will not keep or process data on any individual under the age of 16 years old.

9. Data breaches – We will implement our investigation procedures in the event of a reported or potential data breach.

10. Data Protection by Design and Data Protection Impact Assessments – due to the nature of the works we undertake and the amount and type of data we hold / process. We will not undertake a Data privacy impact assessment (DPIA). However, we will ensure our systems promote privacy by design.

11. Data Protection Officers – The Head of Compliance is designated as the company's data protection officer.

Section 5	Document History
Feb 2018	New Document
May 2018	Inclusion of the GDPR 2018 requirements