

KPH

DECONSTRUCTION

SITE INDUCTION POLICY DOCUMENTS



"Working safely for our future"

CONTENTS

1.	Site Safety Rules	3
2.	Alcohol and Drugs Policy	4
3.	Anti-Bribery and Corruption Policy	5-7
4.	Harassment and Bullying Policy	8-11
5.	Code of Ethics Policy	12-13
6.	Corporate Social Responsibility	14
7.	Data Protection Policy	15-36
8.	Environmental Policy Statement	37
9.	Equality and Diversity Policy	38
10.	Health and Safety Policy	39
11.	Information Security Policy	40-46
12.	Modern Slavery and Human Trafficking Statement	47-48
13.	Non English Speaking Personnel Policy Statement	49
14.	On-Site Mobile Phone Policy	50
15.	Quality Policy Statement	51
16.	Right to work in the UK	52-58
17.	Social Media Policy	59-62
18.	Staff Well-Being Policy	63-65
19.	Sustainable Timber Procurement Policy Statement	66
20.	Whistle-Blowing Policy	67-71
21.	Work Safe Policy Statement	72
22.	Organisational Chart - KpH Deconstruction	73

SITE SAFETY RULES

THE FOLLOWING RULES MUST BE OBEYED AT ALL TIMES.
Failure to do so may result in your removal from site.

- 1) Hard Hats must be worn by all persons on Site. This includes visitors and sub-contractors. Contractors and sub-contractors must ensure that Hard Hats are worn, where necessary, by all their personnel whilst on site.
- 2) The Site must be kept clean at all times, and all rubbish must be cleared away from the work area as soon as practicable.
- 3) All personnel must be properly informed and adequately trained for the work they are employed to carry out.
- 4) Non Speaking “English” site personnel will have a translator available at all times by a foreign national of that language, whom will act as a communicator between them and the site supervisor.
- 5) Personal Protective Equipment and suitable clothing appropriate to the task being carried out must be worn at all times.
- 6) No drugs or alcohol are allowed on Site, and any person who is considered to be under the influence of alcohol or drugs will be removed from Site.
- 7) No smoking or carrying of matches/lighters will be permitted on Site, except in specially designated areas.
- 8) All dust, noise and pollution must be kept to a minimum and measures taken to prevent any nuisance arising from the carrying out of work.
- 9) No explosives or explosive powered equipment may be used on Site.
- 10) No radio transmitters are allowed on Site without written permission.
- 11) No percussion, hammer action tools or vibration equipment is allowed on Site without written permission.
- 12) No visitors, contractors, sub-contractors or their staff will be allowed to remain on Site unless they fully comply with the “Site Access” requirements. Visitors must also be accompanied at all times.
- 13) No unauthorised advertising, publicity or disclosures are allowed.
- 14) No parking on Site, except in areas designated by the Site Supervisor.
- 15) No abusive language, wolf whistling, horse play or unruly behavior on Site.No
- 16) fires on Site.
- 17) Lone working is not permitted on Site.
- 18) All visitors, contractors, sub-contractors and their staff must familiarise themselves with the emergency evacuation procedures on Site.
- 19) Equipment must only be used in the correct manner and for its intended purpose.
- 20) Any procedure, arrangement or restriction imposed by the Site Supervisor or other authorised person must be strictly adhered to.
- 21) The use of mobile phones (Calls, Texting, Music, Facebook and Twitter) and other electronic devices e.g. headphones are restricted to the canteen, rest area or designated compound areas and only during official breaks.
- 22) Any injuries, however minor, shall be reported and recorded in the accident book located in the site office.



Alcohol and Drugs Policy

KpH Group Ltd is committed to providing a safe and secure environment for all persons affected by its work activities. It recognises the inherent risks associated with drug, alcohol and solvent abuse and is intent on safeguarding its workplaces and work activities from these risks. In respect of any person carrying out work at any location on behalf of KpH Group Ltd, the Company has adopted a policy of zero tolerance in that no one shall:

- be in possession of drugs or substances capable of abuse;
- consume or be under the influence of alcohol, drugs or substances of abuse;
- take prescribed drugs without informing their supervisor and having first confirmed with their doctor that the drugs would not affect their fitness for work;
- take medication that carries a warning advising against driving or operating plant or machinery when working;
- trade in or supply alcohol, drugs and substances of abuse, or permit their presence or use by others.

Failure to comply with this policy and the Company's procedures is a serious matter and anyone found to be in breach will be the subject of disciplinary action under the Company's Disciplinary Procedure, which may lead to Summary Dismissal for Gross Misconduct.

It is company policy to always to involve the police where illegal drugs are found to have been used or sold on the premises or on a client's site.


The Company recognises alcohol or drug dependency as a treatable condition. Employees who suspect they have an alcohol or drug dependency are encouraged to seek advice and to follow appropriate treatment promptly before it results in job performance problems.

The Company is not looking to discriminate against employees who approach it for help with a drink or drug related problem and who are prepared to undergo an agreed form of treatment. However, approaches of this nature will not be considered acceptable when they have been made subsequent, or just prior to a Company check that has or would have, revealed recent consumption of alcohol, drugs or substances of abuse or possession of these.

The policy applies to all direct and subcontract employees of KpH Group Ltd and to any other person who carries out work on its behalf. It is designed to protect such persons, visitors and members of the public from the workplace hazards associated with alcohol consumption and drug or solvent abuse. It will be implemented at all UK workplaces and on the instruction of either the Company or joint venture board as appropriate, on overseas operations.

This policy will be brought to the attention of all employees and persons working on behalf of the company and will be reviewed at least annually.

Signed for KpH Group Limited:

Mr Kevin Potter Managing Director	
Date:	03/08/2021



Anti-Bribery and Corruption Policy

1. Introduction

KpH Group Ltd values its reputation and is committed to maintaining the highest level of ethical standards in the conduct of its business affairs. The actions and conduct of the Company's staff as well as others acting on the Company's behalf are key to maintaining these standards.

The purpose of this document is to set out the Company's policy in relation to bribery and corruption. The policy applies strictly to all employees, directors, agents, consultants, contractors and to any other people or bodies associated with the KpH Group Ltd group of companies, within all regions, areas and functions.

2. Understanding and Recognising Bribery and Corruption

Acts of bribery or corruption are designed to influence an individual in the performance of their duty and incline them to act in a way that a reasonable person would consider to be dishonest in the circumstances.

Bribery can be defined as offering, promising or giving a financial (or other) advantage to another person with the intention of inducing or rewarding that person to act or for having acted in a way which a reasonable person would consider improper in the circumstances. Corruption is any form of abuse of entrusted power for private gain and may include, but is not limited to, bribery.

Bribes are not always a matter of handing over cash. Gifts, hospitality and entertainment can be bribes if they are intended to influence a decision.

3. Penalties

The Bribery Act 2010 comes into force on 1 July 2011. Under that Act, bribery by individuals is punishable by up to ten years' imprisonment and/or an unlimited fine. If the firm is found to have taken part in the bribery or is found to lack adequate procedures to prevent bribery, it too could also face an unlimited fine.

A conviction for a bribery or corruption related offence would have severe reputational and/or financial consequences for the Company.

4. KpH Group Ltd's Policy

KpH Group Ltd will not tolerate bribery or corruption in any form.

The Company prohibits the offering, giving, solicitation or the acceptance of any bribe or corrupt inducement, whether in cash or in any other form:

- to or from any person or company wherever located, whether a public official or public body, or a private person or company;
- by any individual employee, director, agent, consultant, contractor or other person or body acting on the firm's behalf;
- in order to gain any commercial, contractual, or regulatory advantage for the firm in any way which is unethical or to gain any personal advantage, pecuniary or otherwise, for the individual or anyone connected with the individual.

This policy is not intended to prohibit the following practices provided they are appropriate, proportionate and are properly recorded:

- normal hospitality, provided that it complies with the Company's Corporate Entertainment Policy;
- fast tracking a process which is available to all on the payment of a fee; and/or
- providing resources to assist a person or body to make a decision more efficiently, provided that it is for this purpose only.

It may not always be a simple matter to determine whether a possible course of action is appropriate. If you are in any doubt as to whether a possible act might be in breach of this policy or the law, the matter should be referred to your Division Manager. If necessary, guidance should also be sought from the Group Commercial Manager and externally appointed HR consultants.

The Company will investigate thoroughly any actual or suspected breach of this policy, or the spirit of this policy. Employees found to be in breach of this policy may be subject to disciplinary action which may ultimately result in their dismissal.

5. Key Risk Areas

Bribery can be a risk in many areas of the Company. Below are the key areas you should be aware of in particular:

Excessive gifts, entertainment and hospitality: can be used to exert improper influence on decision makers. Gifts, entertainment and hospitality are acceptable provided they fall within the Company's Corporate Entertainment Policy.

Facilitation payments: are used by businesses or individuals to secure or expedite the performance of a routine or necessary action to which the payer has an entitlement as of right. The Company will not tolerate or excuse such payments being made.

Reciprocal agreements: or any other form of 'quid pro quo' are never acceptable unless they are legitimate business arrangements which are properly documented and approved by management. Improper payments to obtain new business, retain existing business or secure any improper advantage should never be accepted or made.

Actions by third parties for which the Company may be held responsible: can include a range of people i.e. agents, contractors and consultants, acting on the Company's behalf. Appropriate due diligence should be undertaken before a third party is engaged. Third parties should only be engaged where there is a clear business rationale for doing so, with an appropriate contract. Any payments to third parties should be properly authorised and recorded.


Record keeping: can be exploited to conceal bribes or corrupt practices. We must ensure that we have robust controls in place so that our records are accurate and transparent.

6. Employee Responsibility and How to Raise a Concern

The prevention, detection and reporting of bribery or corruption is the responsibility of all employees throughout the Company. If you become aware or suspect that an activity or conduct which is proposed or has taken place is a bribe or corrupt, then you have a duty to report this.

KpH Group Ltd do not accept gifts, or invites to events, to individually named personnel. In the event that this happens, employees are to refer such matters to their Divisional Manager or Managing Director.

Signed for KpH Group Limited:

Mr Kevin Potter Managing Director	
Date:	03/08/2021



Harassment and Bullying Policy

POLICY

1. KPH Group recognises that all employees have a right to work in an environment in which the dignity of individuals is respected and which is free from harassment and bullying. It is committed to eliminating intimidation in any form.
2. The Policy applies to harassment on the grounds of disability, gender, marital status, sexual orientation, age, creed, colour, race or ethnic origin.
3. Harassment breaches KPH Group Policy as outlined and it is classified as a serious offence which may result in disciplinary action including summary dismissal under the Disciplinary Procedure.
4. The Policy applies to all staff employed by KPH Group.

DEFINITIONS

5. Harassment is generally described as "unwanted conduct which affects the dignity of women or men at work; it encompasses unwelcome physical, verbal or non-verbal behaviour which denigrates or ridicules or is intimidatory". The essential characteristic of harassment is that the action(s) is unwanted by the recipient.
6. The following interpretations and examples of harassment may be helpful in determining whether harassment has taken place.

General Harassment

"Harassment can take many forms and may be directed in particular against women and ethnic minorities or towards people because of their age, disability, gender / gender reassignment, marriage / civil partnership, pregnancy / maternity, race, religion or belief, sex, or sexual orientation. It may involve action, behaviour, comment or physical contact which is found objectionable or which causes offence; it can result in the recipient feeling threatened, humiliated or patronised and it can create an intimidating work environment."

Sexual Harassment

"Sexual harassment can be defined as an uninvited, unreciprocated and unwelcome behaviour of a sexual nature which is offensive to the person involved and causes that person to feel threatened, humiliated or embarrassed. Examples of sexual harassment are:

- requests for sexual favours, including implied or overt promises of preferential treatment or threats concerning present or future employment status;
- offensive gestures or comments;
- sexually-orientated jibes, innuendo or jokes;
- unwanted physical contact;
- the display of sexually offensive visual material such as calendars, photographs,

books or videos.

Sexual harassment may be experienced by men or women as a result of the conduct of men or women. It applies equally regardless of grade or level of job and may also occur when dealing with external clients and/or members of the public".

Racial or Sectarian Harassment

"In the workplace, racial or sectarian harassment may take the form of actual or threatened physical abuse or it may involve offensive jokes, verbal abuse, language, graffiti or literature of a racist or sectarian nature or offensive remarks about a person's skin colour, physical characteristics or religion. It may also include repeated exclusion of a person from an ethnic or religious minority from conversations, patronising remarks, unfair allocation of work or pressure about the speed and/or quality of their work in a way which differs from the treatment of other employees."

Bullying

"Bullying is the intimidation or belittling of someone through the misuse of power or position which leaves the recipient feeling hurt, upset, vulnerable or helpless. It is often inextricably linked to the areas of harassment described above. The following are examples of bullying:

- Unjustified criticism of an individual's personal or professional performance, shouting at an individual, criticising an individual in front of others.
- Spreading malicious rumours or making malicious allegations.
- Intimidation or ridicule of individuals with disabilities and /or learning difficulties.
- Ignoring or excluding an individual from the team / group "

RESPONSIBILITIES OF MANAGERS

7. Every manager has an obligation to prevent harassment / bullying and to take immediate action once it has been identified, whether or not a complaint has been made.
8. Allegations of harassment or bullying, received either informally or formally, must be dealt with promptly and sensitively.
9. It is important that managers recognise that sexual harassment is any sexual advance unwanted by the recipient or behaviour which causes offence to the recipient. Similarly, racial harassment is behaviour which is racially offensive to the recipient. Managers must therefore take care to ensure that they do not pre-judge situations based on their own sexual or racial attitudes and perceptions.
10. It may not always be appropriate for a line manager to be involved with specific complaints. For example, if the complainant is male and wishes to speak to a male, but the manager is female, or, if the complaint relates to the conduct of the line manager. The procedure below sets out the alternatives for such instances.

RESPONSIBILITIES OF ALL EMPLOYEES

11. Every employee has a personal responsibility **NOT** to harass or bully other members of staff.
12. An employee who becomes aware of harassment or bullying occurring should bring the matter to the attention of his/her manager.

REDRESS

13. An employee who feels that he/she has been harassed or bullied has a right to seek redress via the procedures set out below.

PROCEDURE FOR DEALING WITH HARASSMENT

14. An employee who feels that he/she is being subjected to harassment or bullying may attempt to resolve the matter informally in the first instance. In some cases it may be possible and sufficient for him/her to explain clearly to the person(s) engaged in the unwanted activities that the behaviour is unwelcome, that it offends or makes him/her uncomfortable.
 - If at the initial informal discussion stage the circumstances are too difficult or embarrassing to approach the harasser alone, the complainant may wish to be accompanied by a friend or colleague;
 - the complainant may wish to write a letter to the harasser (research has shown this to be very effective);
 - the complainant should keep a record of any incidents, detailing when, where, what occurred, and witnesses (if any);
 - in some cases victims of harassment or bullying may not be sufficiently confident to tell the harasser that his or her behaviour is unacceptable. The Company emphasises therefore that staff **are not required** to approach the harasser in an attempt to resolve the problem informally, and are entitled to report the matter immediately if they so wish.
15. Where the steps outlined above are unsuccessful or inappropriate, the complainant should raise the matter informally and in confidence with his/her manager. Alternatively, the matter may be raised with a more senior manager (if felt necessary this could be of the same sex as the complainant).
16. If the complaint relates to the conduct of the complainant's manager, the complainant may choose to discuss the matter with his/her manager's line manager.
17. The Manager will discuss the matter with the complainant and agree a course of action. The complainant may be accompanied by a representative or work colleague at these meetings. The alleged harasser will also have the right to state their version of events to the manager and to also be accompanied by a representative or colleague.
18. The complainant must be assured that he/she will not be discriminated against or victimised for raising the complaint. Confidentiality will be observed throughout and the need for any disclosure of the details of the case will be discussed and agreed.
19. At any stage of the process the complainant, the manager dealing with the complaint or the accused may feel that they need the help of an independent person before deciding on the best course of action. The Company will seek the advice of a suitable trained persons who can give confidential advice and assistance, including:
 - advising on the nature of harassment;
 - offering guidance on resolving harassment problems, including acting as an independent broker
20. If the situation cannot be resolved informally then the complainant has the right to pursue his or her complaint formally via the Company's Grievance Procedure.

21. Where management consider that there may be evidence of harassment, they may consider it appropriate to undertake a full investigation of the circumstances. In this case a manager not connected with the department involved, or an individual external to the Company will be commissioned to undertake this investigation. Best practice in relation to confidentiality will be maintained during this investigation; and both the complainant and alleged harasser will have the opportunity to have their say. The investigator will also interview and take statements from any appropriate witnesses to the alleged harassment.
22. Where there is evidence that harassment has occurred, prompt and corrective action will be taken, including disciplinary action where appropriate. Harassment is a serious offence which may result in summary dismissal.

COMMUNICATION

23. All staff will be informed of the Harassment and Bullying Policy and Procedure. They must be re-assured regarding:
 - fear that others will consider the behaviour trivial and not take complaints of harassment seriously;
 - fear that no action will be taken against a person guilty of harassment;
 - fear of retaliation or victimisation in registering a complaint either informally or formally through the Grievance Procedure.
24. The Harassment and Bullying Policy will be part of staff induction.

TRAINING

25. Training will be provided for those employees who have a specific responsibility for implementing this Procedure or who may be involved in dealing with complaints which arise.

MONITORING AND REVIEW

26. In order to assess the effectiveness of the Procedure, statistics will be maintained in respect of the complaints of harassment. Strict confidentiality will be maintained and the monitoring process will comply with the Data Protection Act.
27. The effectiveness of this policy will be reviewed regularly.

Signed for KpH Group Limited:

<p>Mr Kevin Potter Managing Director</p>	
<p>Date:</p>	<p>12/10/2021</p>



Code of Ethics Policy

Ethical behaviour underpins the way we behave, do business and treat one other. Our values determine our behaviour and we must support and uphold them so they are an integral part of day to day life in KpH Group Ltd. This policy aims to guide our actions and those of people both with whom we work closely, encouraging a way of working which is honest, responsible and respectful, generating trust.

Purpose

To ensure there is clarity in what is expected of each and every one of us in terms of ethical behaviour.

Scope

This code applies to all employees of KpH and all those working alongside, in partnership and on behalf of KpH.

Policy and Procedures

Every employee of KpH should:

- treat everyone with dignity and respect;
- treat the company's assets and equipment as you would your own;
- operate within the letter and the spirit of law, exercising power and influence responsibly;
- respect the laws and customs in countries in which we operate.

KpH is committed to achieving the highest standards of corporate responsibility in all its business dealings and relationships. This Code of Ethics is underpinned by a number of policies guiding the way we behave, including:

- Code of Professional Conduct
- KpH Supply Chain Code of Conduct
- Equal Opportunities
- Health and Safety
- Sustainable Development
- Information Security
- Socially Responsible Investment
- Whistle Blowing – “Speak Up”

These policies underpin KpH's acceptance of the principles of the Universal Declaration of Human Rights and the International Labour Organisation Conventions. These apply to the management and operation of KpH, and everyone involved. In addition, KpH's Ethics Committee has the role of considering any ethical issues which may arise in the business under this policy.

Compliance


In establishing whether or not any conduct or activity may be in contravention of this code, ask yourself whether:

- It is legal?
- It is in breach of this or any other policies?
- It could be perceived as bringing you, your colleagues or KpH or associated companies into disrepute?
- It could be perceived as compromising you, your colleagues or KpH or associated companies?
- It could be considered by the public as ethical, appropriate and acceptable?

If you are in any doubt, stop and contact either your line manager or any member of Human Resources.

Contravention of this Code could lead to disciplinary action.

Signed for KpH Group Limited:

Mr Kevin Potter Managing Director	
Date:	03/08/2021



Corporate Social Responsibility Statement

KpH Group Ltd acknowledges their responsibilities towards society, the environment and our stakeholders.

Through managing our business in a fair and ethical manner we are able to demonstrate our consideration towards employees and the wider community.

We will provide a safe and healthy working environment for our employees and for visitors to our premises and sites and ensure sufficient information and training is made available in pursuance of their activities.

The ISO standard, to which we are accredited, provides a framework for continuous improvement in our environmental and quality management procedures and performance.


We are committed to managing our impact on the world's natural resources and strive to continually improve our environmental credentials.

We recognise our position within the community and acknowledge that our business activities have varying impacts upon the society in which we operate. We endeavour to manage these in a responsible manner.

We seek to build relationships with our suppliers, customers and stakeholders for mutual benefit and for the benefit of the community.

Through our policies and objective's we will manage our activities and environmental impacts to continuously develop and improve our Corporate Responsibility.

Signed for KpH Group Limited:

Mr Kevin Potter Managing Director	
Date:	03/08/2021



DATA PROTECTION POLICY

FOR:



KPH GROUP LTD

**KPH ENVIRONMENTAL SERVICES LTD
AND KPH DECONSTRUCTION LTD**



AS REQUIRED BY:

GENERAL DATA PROTECTION REGULATIONS

AND

DATA PROTECTION ACT 2018

OFFICE COPY (CONTROLLED DOCUMENT)

DOCUMENT TITLE:	DATA PROTECTION POLICY
DOCUMENT NO:	KpH Data Protection Policy
DATE:	03 AUGUST 2021
ISSUE NO:	4

AMENDMENT RECORD:

Issue No.	Summary of Change	Date	Author	Initialled	Reviewed by
01	First Issue	25/05/2018	Amy Hathaway	AH	LW PB MW SD KP
02	Annual Review	31/08/2019	Steve Dellaway	SD	LW MW KP
03	GDPR Process Additions	21/01/2020	Amy Hathaway	AH	LW SD
04	Annual Review – Legislative Changes	03/08/2021	Lyndsey West	LW	MW KP SD
05					
06					
07					
08					
09					
10					
11					
12					

CONTENTS

1.	INTRODUCTION	4
2.	DATA PROTECTION PRINCIPLES	4
3.	LAWFUL FAIR AND TRANSPARENT DATA PROCESSING	5
4.	PROCESSED FOR SPECIFIED, EXPLICIT AND LEGITIMATE PURPOSES	5
5.	ADEQUATE, RELEVANT AND LIMITED DATA PROCESSING	5
6.	ACCURACY OF DATA AND KEEPING DATA UP TO DATE	5
7.	TIMELY PROCESSING	6
8.	SECURE PROCESSING	6
9.	ACCOUNTABILITY	6
10.	PRIVACY IMPACT ASSESSMENT	6
11.	THE RIGHTS OF DATA SUBJECTS	7
12.	KEEPING DATA SUBJECTS INFORMED	7
13.	DATA SUBJECT ACCESS REQUEST (SAR)	8
14.	RECTIFICATION OF PERSONAL DATA	9
15.	ERASURE OF PERSONAL DATA (“REQUEST TO BE FORGOTTEN”)	9
16.	RESTRICTION OF PERSONAL DATA PROCESSING	10
17.	DATA PORTABILITY	10
18.	OBJECTIONS TO PERSONAL DATA PROCESSING	10
19.	AUTOMATED DECISION-MAKING	11
20.	PROFILING	11
21.	PERSONAL DATA	12
22.	DATA PROTECTION MEASURES	12
23.	ORGANISATIONAL MEASURES	14
24.	TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA	14
25.	DATA BREACH NOTIFICATION	15
26.	IMPLEMENTATION OF POLICY	16
	APPENDIX 1 - DEFINITIONS	17
	APPENDIX 2 – WORKFLOW PROCESS: SUBJECT ACCESS REQUEST (SAR)	20
	APPENDIX 3 – WORKFLOW PROCESS: REQUEST TO BE FORGOTTEN	21
	APPENDIX 4 – WORKFLOW PROCESS: DATA BREACH	22

1. INTRODUCTION

- 1.1 This Policy sets out the obligations of KpH Group Ltd (“the Company”) regarding data protection and the rights of direct employees, agency staff, customers, sub-contractors, business contacts, members of the public (“data subjects”) in respect of their personal data under the UK-GDPR and 2018 Data Protection Regulation (“the Regulation”).
- 1.2 The Regulation defines “personal data” as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
- 1.3 This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.
- 1.4 The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. DATA PROTECTION PRINCIPLES

- 2.1 This Policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling personal data must comply. All personal data must be:
 - a) processed lawfully, fairly, and in a transparent manner in relation to the data subject;
 - b) collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
 - c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
 - d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;
 - e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject;
 - f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3. LAWFUL FAIR AND TRANSPARENT DATA PROCESSING

- 3.1 The Regulation seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The Regulation states that processing of personal data shall be lawful if at least one of the following applies:
- a) the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;
 - b) processing is **necessary for the performance of a contract** to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
 - c) processing is necessary for **compliance with a legal obligation** to which the controller is subject;
 - d) processing is necessary to **protect the vital interests of the data subject** or of another natural person;
 - e) processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller;
 - f) processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4. PROCESSED FOR SPECIFIED, EXPLICIT AND LEGITIMATE PURPOSES

- 4.1 The Company collects and processes the personal data set out in Part 21 of this Policy. This may include personal data received directly from data subjects (for example, contact details used when a data subject communicates with us) and data received from third parties (for example, contact details or training records from a Sub-Contractor).
- 4.2 The Company only processes personal data for the specific purposes set out in Part 21 of this Policy (or for other purposes expressly permitted by the Regulation). The purposes for which we process personal data will be informed to data subjects at the time that their personal data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

5. ADEQUATE, RELEVANT AND LIMITED DATA PROCESSING

- 5.1 The Company will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Part 4, above.

6. ACCURACY OF DATA AND KEEPING DATA UP TO DATE

- 6.1 The Company shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data shall be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

7. TIMELY PROCESSING

- 7.1 The Company shall not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it without delay.

8. SECURE PROCESSING

- 8.1 The Company shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in Parts 22 and 23 of this Policy.

9. ACCOUNTABILITY

- 9.1 The Company's Data Protection Manger is Steve Dellaway and his contact details are Telephone: 01883 346604 and Email: steve.dellaway@kph.co.uk.
- 9.2 The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:
- a) The name and details of the Company, its Data Protection Manager, and any applicable third-party data controllers.
 - b) The purposes for which the Company processes personal data.
 - c) Details of the categories of personal data collected, held, and processed by the Company; and the categories of data subject to which that personal data relates.
 - d) Details (and categories) of any third parties that will receive personal data from the Company.
 - e) Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards.
 - f) Details of how long personal data will be retained by the Company.
 - g) Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

10. PRIVACY IMPACT ASSESSMENT

- 10.1 The Company shall carry out Privacy Impact Assessments when and as required under the Regulation. Privacy Impact Assessments shall address the following areas of importance:
- a) The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data.
 - b) Details of the legitimate interests being pursued by the Company.
 - c) An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed.

- d) An assessment of the risks posed to individual data subjects.
- e) Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation.

11. THE RIGHTS OF DATA SUBJECTS

11.1 The Regulation sets out the following rights applicable to data subjects:

- a) The right to be informed.
- b) The right of access.
- c) The right to rectification.
- d) The right to erasure (also known as the 'right to be forgotten').
- e) The right to restrict processing.
- f) The right to data portability.
- g) The right to object.
- h) Rights with respect to automated decision-making and profiling.

12. KEEPING DATA SUBJECTS INFORMED

12.1 The Company shall ensure that the following information is provided to every data subject when personal data is collected:

- a) Details of the Company including, but not limited to, the identity it's Data Protection Manager.
- b) The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 21 of this Policy) and the legal basis justifying that collection and processing.
- c) Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data.
- d) Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed.
- e) Where the personal data is to be transferred to one or more third parties, details of those parties.
- f) Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 24 of this Policy for further details concerning such third country data transfers).
- g) Details of the length of time the personal data will be held by the Company (or, where there is no predetermined period, details of how that length of time will be determined).
- h) Details of the data subject's rights under the Regulation.

- i) Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time.
 - j) Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the Regulation).
 - k) Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it.
 - l) Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.
- 12.2 The information set out above in Part 12.1 shall be provided to the data subject at the following applicable time:
- 12.3 Where the personal data is obtained from the data subject directly, at the time of collection;
- 12.4 Where the personal data is not obtained from the data subject directly (i.e. from another party):
- a) If the personal data is used to communicate with the data subject, at the time of the first communication; or
 - b) If the personal data is to be disclosed to another party, before the personal data is disclosed; or
 - c) In any event, not more than one month after the time at which the Company obtains the personal data.

13. DATA SUBJECT ACCESS REQUEST (SAR)

- 13.1 A data subject may make a subject access request ("SAR") at any time to find out more about the personal data which the Company holds about them. The Company is normally required to respond to SARs within 28 days of receipt (this can be extended by up to 56 days in the case of complex and/or numerous requests, and in such cases, the data subject must be informed of the need for the extension).
- 13.2 All subject access requests received must be forwarded to Steve Dellaway, the Company's Data Protection Manager (steve.dellaway@kph.co.uk), to process the request and record the outcome on the **Access Log**.
- 13.3 The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

13.4 Please see **Appendix B** for a Workflow Process Diagram on Subject Access Requests (SAR).

14. RECTIFICATION OF PERSONAL DATA

- 14.1 If a data subject informs the Company that personal data held by the Company is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt the data subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).
- 14.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.

15. ERASURE OF PERSONAL DATA ("REQUEST TO BE FORGOTTEN")

- 15.1 Data subjects may request that the Company erases the personal data it holds about them (otherwise known as a "request to be forgotten") in the following circumstances:
- a) It is no longer necessary for the Company to hold that personal data with respect to the purpose for which it was originally collected or processed.
 - b) The data subject wishes to withdraw their consent to the Company holding and processing their personal data.
 - c) The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 18 of this Policy for further details concerning data subjects' rights to object).
 - d) The personal data has been processed unlawfully.
 - e) The personal data needs to be erased in order for the Company to comply with a particular legal obligation.
- 15.2 The Data Protection Manager must be notified of the request so that arrangements can be made for the request to be processed within the appropriate timeframe and recorded on the Request to be Forgotten Log.
- 15.3 Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within 28 days of receipt of the data subject's request (this can be extended by up to 56 days in the case of complex requests; however, in such cases, the data subject must be informed of the need for the extension).
- 15.4 In the event that any personal data that is to be erased (in response to a data subject request) has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).
- 15.5 Please see **Appendix C** for a Workflow Process Diagram on Requests to be Forgotten.

16. RESTRICTION OF PERSONAL DATA PROCESSING

- 16.1 Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.
- 16.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17. DATA PORTABILITY

- 17.1 Where data subjects have given their consent to the Company to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between the Company and the data subject, data subjects have the legal right under the Regulation to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers e.g. other organisations).
- 17.2 To facilitate the right of data portability, the Company shall make available all applicable personal data to data subjects in the following format[s]:
- a) electronic;
 - b) as requested.
- 17.3 Where technically feasible, if requested by a data subject, personal data shall be sent directly to another data controller.
- 17.4 All requests for copies of personal data shall be complied with within one month of the data subject's request (this can be extended by up to two months in the case of complex requests in the case of complex or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

18. OBJECTIONS TO PERSONAL DATA PROCESSING

- 18.1 Data subjects have the right to object to the Company processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling), [and processing for scientific and/or historical research and statistics purposes].
- 18.2 Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing forthwith, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.
- 18.3 Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing forthwith.
- 18.4 Where a data subject objects to the Company processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the Regulation, 'demonstrate grounds relating to his or her particular situation'. The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

19. AUTOMATED DECISION-MAKING

19.1 In the event that the Company uses personal data for the purposes of automated decision-making and those decisions have a legal (or similarly significant effect) on data subjects, data subjects have the right to challenge to such decisions under the Regulation, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the Company.

19.2 The right described in Part 19.1 does not apply in the following circumstances:

- a) The decision is necessary for the entry into, or performance of, a contract between the Company and the data subject.
- b) The decision is authorised by law.
- c) The data subject has given their explicit consent.

20. PROFILING

20.1 Where the Company uses personal data for profiling purposes, the following shall apply:

- a) Clear information explaining the profiling will be provided, including its significance and the likely consequences.
- b) Appropriate mathematical or statistical procedures will be used.
- c) Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected shall be implemented; and
- d) All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 22 and 23 of this Policy for more details on data security).

21. PERSONAL DATA

21.1 The following personal data may be collected, held, and processed by the Company:

Data Category	Reason the Data Collected, Held and Processed
Marketing	Information is collected to keep current and prospective clients up to date with our services, work and achievements.
Accounts	Information is collected to process payroll and financial transactions.
Health and Safety	Information is collected and shared as required to maintain regulation Health and Safety standards and practices.
Human Resources	Information is collected and processed to manage staff contracts and welfare.
Operations	Information is collected, shared and distributed to maintain health and safety standards and carry out our services as contracted.
Quality	Information is processed to meet Quality standards, maintain health and safety practices and evidence compliance with industry regulations.
Tendering	Information is presented to potential clients, providing evidence of our standards and experience, to win work.
Yard	Information is collected and processed to manage the assets and equipment movement in the yard and maintain appropriate Health and Safety standards.

21.2 Please see our **Document Longevity Retention Matrix** for a comprehensive list of personal data and full descriptive details.

22. DATA PROTECTION MEASURES

22.1 The Company shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:

- a) All emails containing personal data must be encrypted using Office365 mail encryption services.
- b) Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded, and electronic copies should be deleted securely using S Delete or Windows Cipher.
- c) Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances.
- d) Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable.
- e) Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data.
- f) Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent in the post by recorded delivery, marked private and confidential.

- g) No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from Steve Dellaway, Data Protection Manager.
- h) All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar.
- i) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of Data Protection Manger, Steve Dellaway (Email: steve.dellaway@kph.co.uk).
- j) Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time.
- k) If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it.
- l) No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the Company or otherwise [without the formal written approval of Data Protection Manger, Steve Dellaway (Email: steve.dellaway@kph.co.uk) and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary].
- m) No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Regulation (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken.
- n) All personal data stored electronically should be backed up daily onsite and offsite. All backups should be encrypted using AES encryption.
- o) All electronic copies of personal data should be stored securely using passwords and AES data encryption.
- p) All passwords used to protect personal data must comply with the company's **Information Security Policy**.
- q) Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords.
- r) Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the Business Development and Quality Co-Ordinator to ensure that no data subjects have added their details to any marketing preference databases including, but not limited to, the Telephone Preference Service, the Mail Preference Service, the Email Preference Service, and the Fax Preference Service. Such details should be checked as and when required.

23. ORGANISATIONAL MEASURES

- 23.1 The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:
- a) All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the Regulation and under this Policy, and shall be provided with a copy of this Policy.
 - b) Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company.
 - c) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so.
 - d) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised.
 - e) Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed.
 - f) The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed.
 - g) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract.
 - h) All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the Regulation.
 - i) Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

24. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

- 24.1 The Company may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.
- 24.2 The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:
- a) The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data.

- b) The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the Regulation); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.
- c) The transfer is made with the informed consent of the relevant data subject(s).
- d) The transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject).
- e) The transfer is necessary for important public interest reasons.
- f) The transfer is necessary for the conduct of legal claims.
- g) The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent.
- h) The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

25. DATA BREACH NOTIFICATION

- 25.1 All personal data breaches must be reported immediately to the Company's Data Protection Manager for investigation and recording on the Data Breach Log.
- 25.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Manager must ensure that the Information Commissioner's Office (ICO) is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
- 25.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 25.2) to the rights and freedoms of data subjects, the Data Protection Manager must ensure that all affected data subjects are informed of the breach directly and without undue delay.
- 25.4 Please see **Appendix D** for a Workflow Process Diagram on Data Breaches.


25.5 Data breach notifications shall include the following information:

- a) The categories and approximate number of data subjects concerned.
- b) The categories and approximate number of personal data records concerned.
- c) The name and contact details of the Company's Data Protection Manager (or other contact point where more information can be obtained).
- d) The likely consequences of the breach.
- e) Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

26. IMPLEMENTATION OF POLICY

26.1 This Policy shall be deemed effective as of 25 May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name:	Mr Kevin Potter
Position:	Managing Director
Date:	03/08/2021
Due for Review by:	02/08/2022
Signature:	

In case of any queries or questions in relation to this policy please contact us info@kph.co.uk.

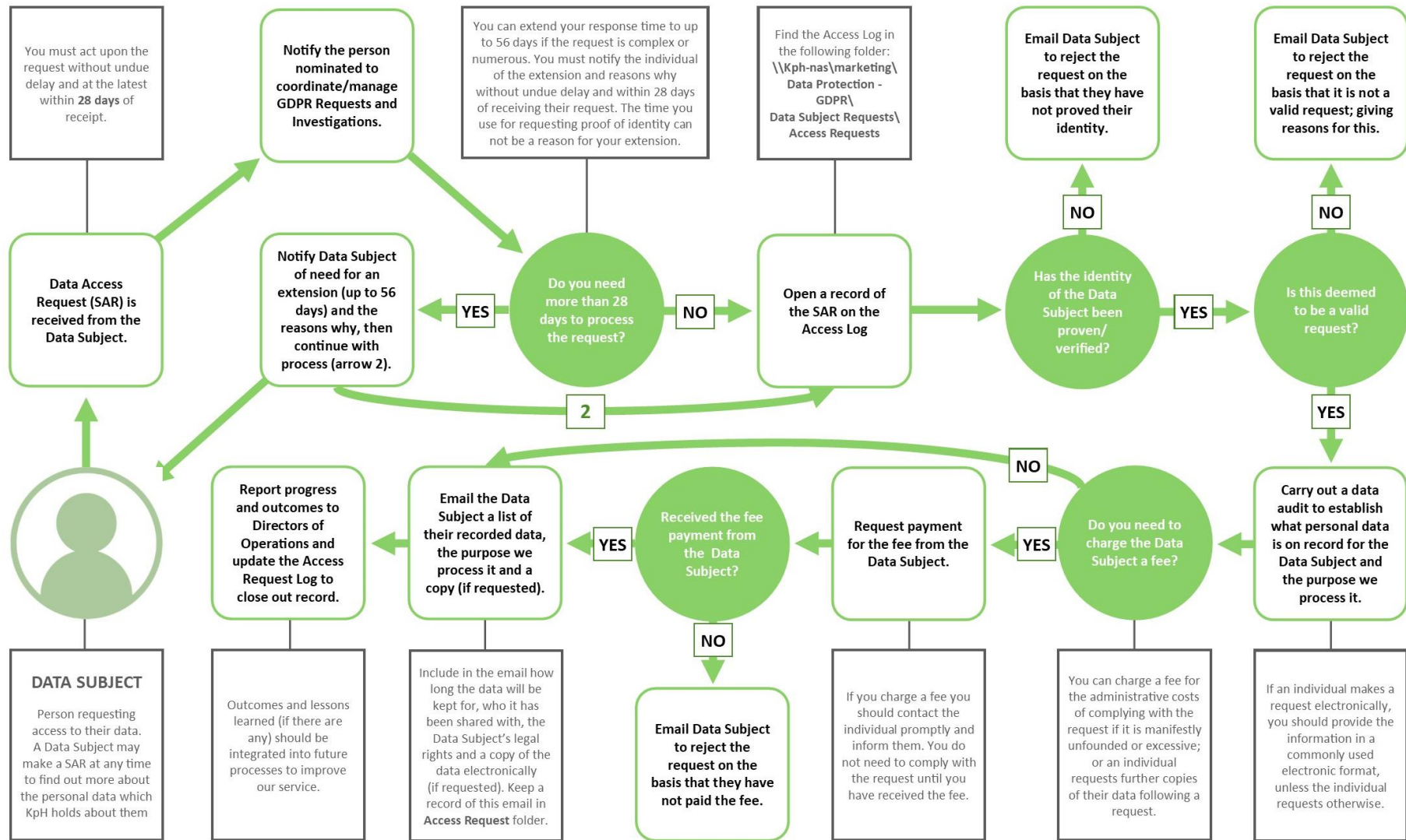
APPENDIX 1 - DEFINITIONS

- (1) **'personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- (2) **'processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- (3) **'restriction of processing'** means the marking of stored personal data with the aim of limiting their processing in the future;
- (4) **'profiling'** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
- (5) **'pseudonymisation'** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
- (6) **'filing system'** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
- (7) **'controller'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- (8) **'processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- (9) **'recipient'** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the 4.5.2016 L 119/33 Official Journal of the European Union EN framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
- (10) **'third party'** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
- (11) **'consent'** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

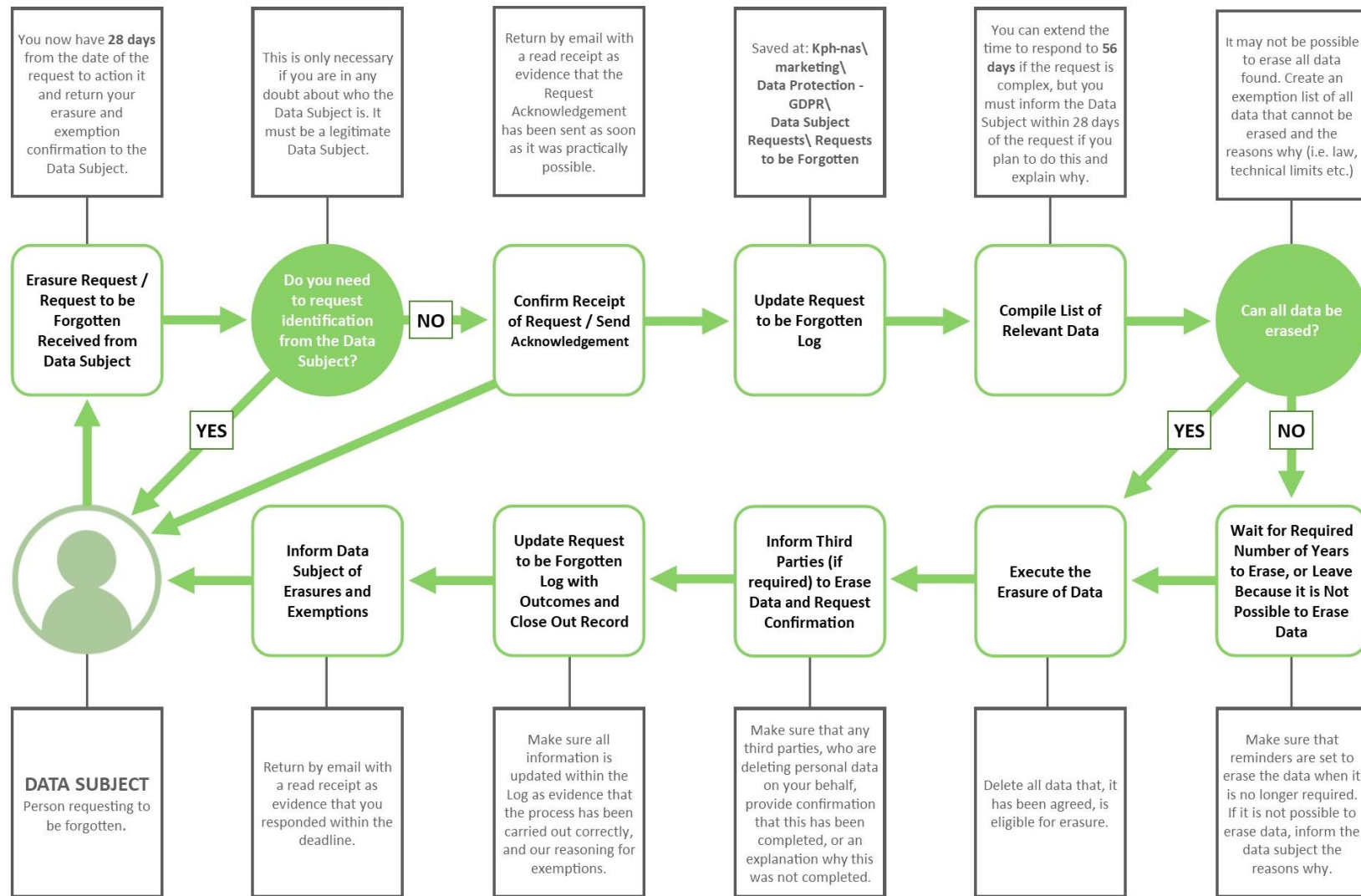
- (12) **‘personal data breach’** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- (13) **‘genetic data’** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
- (14) **‘biometric data’** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
- (15) **‘data concerning health’** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
- (16) **‘main establishment’** means:
- a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;
 - b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;
- (17) **‘representative’** means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;
- (18) **‘enterprise’** means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;
- (19) **‘group of undertakings’** means a controlling undertaking and its controlled undertakings;
- (20) **‘binding corporate rules’** means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;
- (21) **‘supervisory authority’** means an independent public authority which is established by a Member State pursuant to Article 51; 4.5.2016 L 119/34 Official Journal of the European Union EN;

- (22) **‘supervisory authority concerned’** means a supervisory authority which is concerned by the processing of personal data because:
- a) the controller or processor is established on the territory of the Member State of that supervisory authority;
 - b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or
 - c) a complaint has been lodged with that supervisory authority;
- (23) **‘cross-border processing’** means either: (a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.
- (24) **‘relevant and reasoned objection’** means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;
- (25) **‘information society service’** means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (1);
- (26) **‘international organisation’** means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

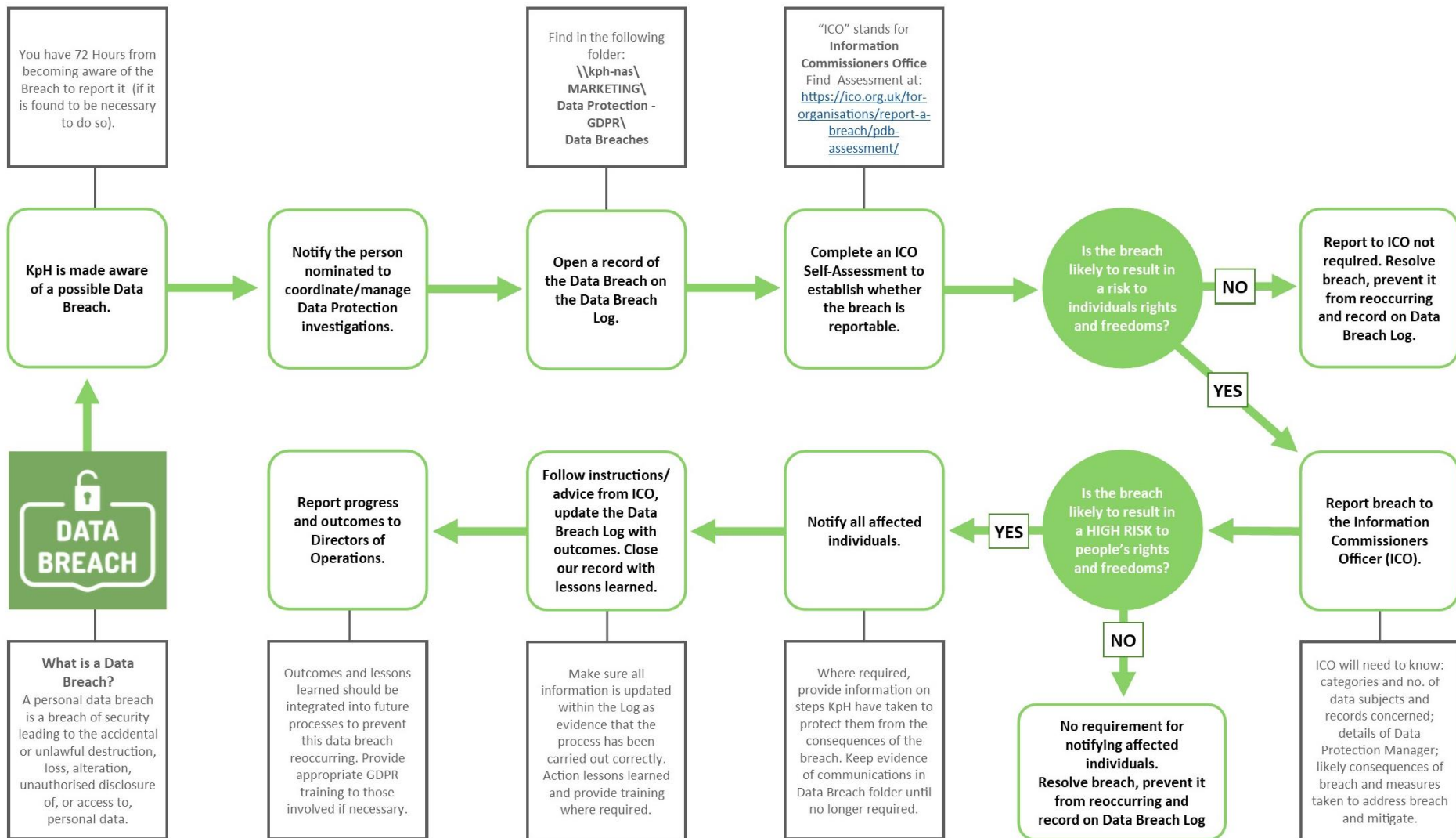
APPENDIX 2 – WORKFLOW PROCESS: SUBJECT ACCESS REQUEST (SAR)



APPENDIX 3 – WORKFLOW PROCESS: REQUEST TO BE FORGOTTEN



APPENDIX 4 – WORKFLOW PROCESS: DATA BREACH





Environmental Policy Statement

KpH Group Limited is committed to high standards of performance in relation to the Environment. In performing our duties our goal is to protect people, minimise harm to the Environment, integrate biodiversity considerations and reduce disruption to our neighbouring communities. KpH also strive to achieve continuous improvement in our Environmental performance.

KpH has established an Environmental Management System based on the requirements of ISO 14001:2015 to ensure that:

- The Management team are committed to the Prevention of Pollution and Protecting the Environment.
- We organise and plan for the Environment efficiently and effectively.
- We aim to minimise discharges, emissions and waste that adversely affect the Environment.
- Staff are given appropriate training to perform their tasks competently, safely and with due regard for the Environment.
- Risks to the Environment from our activities are assessed and either eliminated or reduced to acceptable levels.
- We comply with all applicable Environmental legislation and regulations and apply responsible standards where the legislation is inadequate or non-existent.
- We are comprehensively prepared to respond effectively in the event of an emergency.
- We promote a culture of reporting and investigating accidents, incidents, near misses and the sharing of lessons learned.
- We have an audit programme which verifies compliance with this policy and monitors our Environmental performance.
- Top Management will regularly set and review our Environmental objectives & targets, with the aim of driving continuous improvement in Environmental knowledge and performance.
- This policy is reviewed periodically to ensure its ongoing suitability and effectiveness.

Everyone in KpH has individual authority, responsibility and accountability for protecting the Environment.

Signed for KpH Group Limited:

Mr Kevin Potter Managing Director	
Date:	03/08/2021



Equality and Diversity Policy

Embracing equality has been central to the way we deliver services. KpH Group aim is to promote a safe, supportive and welcoming workplace with values, respect and diversity so people can achieve maximum potential. Considering the needs of our employees and customers in the decisions we have to make as an organisation is vital.

Maintaining a Corporate and Professional Commitment to Equality Issues

We aim to review our Equality scheme annually to ensure that the goals we have set using our action plan at the beginning of the year continue to be relevant priorities for us both as an employer and a service provider.

Having discussions with our clients about our current scheme helps to identify a number of areas where updates need to be made. These updates will be concluded in our action plan.

Equality within our organisation continues to start from the top with our Managing Director identified as the corporate leader for Equality. Senior Managers are informed on any equality implications with reports being presented.

Senior Managers also have the responsibility for overseeing activities and progress in regards to equality. Legislative changes are kept up to date in order to ensure best practice which has an effect on our organisation, employees and our customers.

Every employee is required to adhere to our policy and rules relating to equal opportunity. Any breaches of this policy are dealt with through the disciplinary procedure.

A requirement is placed on our contractors to follow our equality principles and values in order to prove they are demonstrating to us they are meeting the requirements that we have set out.

Training

As an organisation we recognise that training and raising awareness is vital to ensure that our employees understand our Equality principles and that this is reflected in their behaviour.

We ensure all members of staff receive basic training on Equality and Diversity which covers both legal obligations and good practice.

All employees undertake this training on their first week with the company and as a minimum of every 3 years after this. The training provides an overview of the rules and legislation surrounding Equality and Diversity.

Signed for KpH Group Limited:

Mr Kevin Potter Managing Director	
Date:	03-08-2021



Health and Safety Policy Statement

KpH Group (Also called The Company) will take all reasonably practical precautions to ensure the health and safety at work of its employees whether at the Company premises or when carrying out its business elsewhere and also recognise that a duty of care extends to other persons whilst they are on Company premises.

KpH Group Ltd is committed to the continuous improvement of health and safety performance.

The responsibility for safety at work belongs to all Company employees be they upper management, Managers, or operatives and to employees of contractors variously employed.

The Company through its employees also accepts responsibility for the health and safety of others affected by its actions.

To achieve these aims the company will:


- Provide a safe working environment in the operation and maintenance of all plant, equipment and facilities.
- Establish a Safe System of Work (SSOW).
- Ensure that all persons are competent to perform the duties expected of them.
- Provide information, instruction, training, and supervision where appropriate.
- Co-operate with their clients, employees, sub-contractors and others with an interest in health and safety.
- Ensure safety arrangements are in place for the use, handling, storage and transportation of articles and substances.
- Provide a safe place of work including access and egress.
- Ensure that there are adequate resources available to ensure safety is not compromised to ensure adequate training and Personal Protective Equipment is provided.

The Company expects employees to conform to this policy and with The Health and Safety at Work etc.. Act 1974 and to exercise all reasonable care for their own health and safety and that of others who may be affected by their acts or omissions.

This policy and the way it has operated will be reviewed annually to reflect any changes in the nature and size of the business or new or amended legislation.

The Managing Director has ultimate authority and responsibility in relation to all health and safety topics affecting The Company.

The Company employs Bernard Sims Associates of York House, 38-42 Chertsey Street, Guildford, Surrey, GU1 4HD as Health and Safety Consultants.

Signed:		Position:	Managing Director
Name:	Kevin Potter	Date:	19/10/2021



INFORMATION SECURITY POLICY

Table of Content

1	MOTIVATION	2
2	PURPOSE	2
3	SCOPE	2
4	POLICY	2
4.1	GUIDELINES FOR VISITOR ACCESS	2
4.2	GUIDELINES FOR PHYSICAL SECURITY	3
4.3	PASSWORD POLICY	3
4.4	GUIDELINES FOR MEDIA DISPOSAL AND RECYCLING	4
4.5	GUIDELINES FOR UNATTENDED WORKSTATIONS	4
4.6	GUIDELINES FOR WORKING FROM HOME	4
4.7	DATA TYPES	5
4.8	DATA CLASSIFICATIONS	5
5	SUMMARY	6
6	ACKNOWLEDGEMENT OF INFORMATION SECURITY POLICY	6
7	REVIEW	6
8	PROCEDURE	6
9	SIGNATURE	7

1 MOTIVATION

- 1.1.1 The information owned and used to operate KpH Group Ltd required a substantial investment in human and financial resources to develop. The intellectual property and information assets of the company are all valuable company resources and need to be properly protected.
- 1.1.2 To help KpH Group Ltd maintain acceptable information security protection, all employees are responsible for following the steps outlined in this Information Security Policy.

2 PURPOSE

2.1.1 The purpose of this policy is to create a KpH Group Ltd standard for:

- Visitor Access
- Physical Security
- Password Policy
- Media Disposal and Recycling
- Unattended Workstations
- Safe Keeping of Data

3 SCOPE

3.1.1 Everyone who has visitors coming to see them at KpH Group Ltd ("The Company") premises, or who has access to any non-public company information, is expected to follow the guidelines outlined in this policy. This includes people who have access to Company customer database, sales and marketing plans, designs and patents, financial records, any other business information not in the public domain and customer data.

4 POLICY

4.1 GUIDELINES FOR VISITOR ACCESS

4.1.1 Access to company information is restricted to Company employees who require access to perform their jobs. Visitors can present a security risk because there is an opportunity for intentional or unintentional access to confidential information. To manage this risk, visitors and staff should be aware of the following requirements:

- All visitors must report to the main reception desk on arrival.
- All visitors are required to sign in at reception in the Visitors' Register.
- No visitors are allowed to walk around unaccompanied. All visitors must be met at reception by the person they have come to see.
- No pets are permitted. However, assistance animals such as guide dogs are permitted.
- As a rule, visitors are not permitted to take photographs. Exceptions might be made, with the permission of the Company Director, where photographs are required for documentation, auditing or marketing purposes.
- Visitors should not be given information that does not pertain to the reason for their visit. Requests for inappropriate or confidential information should be reported immediately to the Company Director.
- On departure, visitors should sign out at reception in the Visitors' Register.

- In the event of an emergency, employees must ensure that their visitors remain in the evacuation marshalling area.
- Consultants or other visitors requiring Internet network access can use the guest network, if access is required to the company network and any shared resources they will need access set up by the IT Consultant.

4.2 GUIDELINES FOR PHYSICAL SECURITY

4.2.1 It is company policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorised access and environmental hazards. Employees and contractors should be aware that:

- Software and hardware should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields. In addition, hazards such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided.
- Critical computer equipment such as file servers should be protected by an uninterruptible power supply (UPS) and other computer equipment protected by a surge suppressor.
- Software, important data and other confidential information should be stored out of sight when not in use.
- Company equipment such as laptop computers should not be taken off the premises without the consent of their department Manager. The Manager should know what equipment is leaving, what data is on it, and for what purpose it will be used.
- Employees and contractors should exercise care to safeguard the valuable electronic equipment assigned to them. Employees and contractors who neglect this duty may be accountable for any loss or damage that may result.
- Critical equipment, like the server room, should be locked at all times, with access limited to a few authorised key-holders.

4.3 PASSWORD POLICY

4.3.1 The company has a strict password policy which must be adhered to at all times.

- Passwords must be a minimum of 8 characters, there is no maximum length.
- Passwords need to include at least one of the following: 1 Upper case, 1 Lower case, 1 Number and one Special Character.
- Your password should be memorable to you and It is not recommended to use the same password for home and work, additionally you:
 - should avoid using obvious passwords such as those based on easily discoverable information, such as pets and family members;
 - should also avoid using common passwords.
- Two-Factor Authentication will be used where possible and practicable.
- Passwords are required to be inputted correctly before any access is granted to company resources.
- We do not enforce a password expiry, however If you suspect your password is compromised you should immediately change your password and advise you Line Manager.
- Passwords inputted incorrectly will result in your account being locked out and this may require an Administrator to unlock your account after verification.
- If Passwords are recorded they must be stored in an encrypted form.

4.4 GUIDELINES FOR MEDIA DISPOSAL AND RECYCLING

4.4.1 To ensure that confidential company information is not left on various media that the company no longer needs, these guidelines should be followed:

- No media such as old computers, hard drives, USB drives, Flash drives, backup media, CDs and DVDs should be discarded without first removing the data from the media as cleanly as possible.
- All old media to be disposed or recycled should be handed to the IT Consultant.
- The IT Consultant will be responsible for cleaning any data from media to be disposed of, by using hardware and software tools available to properly erase hard drives and USB devices before discarding them.

4.5 GUIDELINES FOR UNATTENDED WORKSTATIONS

4.5.1 A clear desk and clear screen policy helps to create a culture of security awareness among employees and to prevent opportunistic access to confidential information. When away from their desks for meetings, or toilet or lunch breaks, all staff and contractors working at the Company should:

- Lock all papers and other media containing sensitive or confidential information away in a drawer or cabinet.
- Lock their computer screens and ensure computers require a password on resuming working.
- Clear desks and tidy away all papers before going home at the end of each day.
- Get into the habit of locking drawers and filing cabinets at the end of each day and when away from their workstations for extended periods.

4.6 GUIDELINES FOR WORKING FROM HOME

4.6.1 The employee must carry out his/her work for the Company in a room used only for that purpose and must not allow members of his/her family, or third parties who are not employed by the Company, to access or use the Company equipment.

4.6.2 An employee who works at home must agree to not smoke in the room where the work is carried out.

4.6.3 Employees who work at home are responsible for keeping all documents and information associated with the Company's business secure at all times. Specifically, the employee is under a duty to:

- keep filing cabinets and drawers locked when they are not being used;
- keep all documentation belonging to the Company under lock and key at all times except when in use; and,
- set up and use a unique password for the computer.

4.6.4 The computer [and other equipment] provided by the Company for the employee must only be used for work-related purposes and must not be used by any other member of the family at any time, or for any purpose.

4.7 DATA TYPES

4.7.1 The Company deals with two main kinds of data:

- a) **Company-Owned Data** that relates to such areas as corporate financials, employment records, payroll, etc.
- b) **Private Data** that is the property of our clients and/or employees, such as social security numbers, bank account details, contact information, client network access passwords, etc.

4.8 DATA CLASSIFICATIONS

4.8.1 Company data is comprised of the following classifications of information:

1. **Public/Unclassified:** This is defined as information that is generally available to anyone within or outside of the company. Access to this data is unrestricted, may already be available and can be distributed as needed. Public/unclassified data includes, but is not limited to, marketing materials, annual reports and corporate financials.

Employees may send or communicate a public/unclassified piece of data with anyone inside or outside of the company.

2. **Private:** This is defined as corporate information that is to be kept within the company. Access to this data may be limited to specific departments and cannot be distributed outside of the workplace. Private data includes, but is not limited to, work phone directories, organisational charts, company policies, client lists.

All information not otherwise classified will be assumed to be Private.

Employees may not disclose private data to anyone who is not a current employee of the company.

3. **Confidential:** This is defined as personal or corporate information that may be considered potentially damaging if released and is only accessible to specific groups [e.g. payroll, HR, Support, etc]. Confidential data includes, but is not limited to, social security numbers, contact information, tax forms, accounting data, security procedures, server access details. The company considers it a top priority to protect the privacy of our clients and employees.

Employees may only share confidential data within the department or named distribution list.

4. **Secret/Restricted:** This is defined as sensitive data which, if leaked, would be harmful to the company, its employees, contractors and clients. Access is limited to authorised personnel and third parties as required. Secret/restricted data includes but is not limited to client data, audit reports, legal documentation, business strategy details, access details, machine information, client security audits and reports.

Secret/restricted data cannot be disclosed by anyone other than the original author, owner or distributor.

It is the responsibility of everyone who works at the company to protect our data. Even unintentional abuse of classified data will be considered punishable in accordance with the extent and frequency of the abuse.

5 SUMMARY

- 5.1.1 This aim of this **Information Security Policy** is to secure the company's IT resources, and to enable the company to achieve its business objectives. Full co-operation with this **Information Security Policy** is an expected job requirement.

6 ACKNOWLEDGEMENT OF INFORMATION SECURITY POLICY

- 6.1.1 This forms an official acknowledgement by company employees that they have read and understood the company's **Information Security Policy** and agree to follow the guidelines outlined herein.

7 REVIEW

- 7.1.1 Management is responsible for keeping this policy current.
- 7.1.2 This policy will be reviewed annually or as circumstances arise.
- 7.1.3 A full security audit will be performed by the Quality Team annually to ensure that the policy is properly aligned with company directives, Data Protection Policy and Information Governance.

Last Reviewed: 31 July 2020

8 PROCEDURE

- 8.1.1 Complete the following steps:
- Read the **Information Security Policy**.
 - Ask questions or request clarification if anything is unclear.
 - Sign and date this page in the appropriate spaces below.
 - Return this page only to the Quality Manager.

9 SIGNATURE

9.1.1 This agreement is between the undersigned employee and KpH Group Ltd (“The Company”). In signing below, I agree to the following:

- I have received and read a copy of the company’s **Information Security Policy** and understand the contents.
- I understand that adhering to the guidelines outlined in the company’s **Information Security Policy** is part of my job requirement as an employee of the company, and agree to do so.
- I understand and agree to adhere to the **Password Policy** and will not disclose my password to anybody and in the event that I suspect my password may have been compromised will immediately change my password and notify my Line Manager.
- I understand and agree that any computers, software, and storage media provided to me by the company contain proprietary and confidential information about the company, and its customers or vendors, and that this information remains the property of the company at all times.
- I agree that I shall not copy, duplicate (except for back-up purposes as part of my job at the company) or otherwise disclose, or allow anyone else to copy or duplicate any of this information.
- I agree that if I leave the company for any reason, I shall immediately return the original and copies of any and all software, computer equipment and materials that I may have received from the company.
- I understand that failure to observe these guidelines could result in disciplinary action by the company depending upon the type and severity of the violation, whether it causes any liability or loss to the company, and/or the presence of any repeated violation(s).

Mr Kevin Potter Managing Director	
Date:	03/08/2021



Modern Slavery and Human Trafficking Statement

Company Structure

KpH Deconstruction Services Ltd, a member of the KpH Group is a Demolition Company involved in Deconstruction and Demolition. KpH operates predominantly within the M25 but can mobilise to anywhere within the UK. KpH Group Ltd has circa 100 members of staff and has an annual turnover of £12m.

We work closely with a number of suppliers and subcontractors, the majority of whom operate within the UK, so we believe, together with the steps set out below, this mitigates our risk.

Statement

We are committed to ensuring that there is no modern slavery or human trafficking in our supply chains or in any part of our business. This Anti-slavery Statement reflects our commitment to acting ethically and with integrity in all our business relationships and to implementing and enforcing effective systems and controls to ensure slavery and human trafficking is not taking place anywhere in our business or our supply chains.

In order to ensure all those in our supply chain comply with our values, we require our supply chain to contractually commit to compliance with this Statement.

Our recruitment processes are both transparent and thorough. We have robust procedures in place for vetting new employees and ensuring we are able to accurately confirm their identities.

Due Diligence

As part of KpH's on-going commitment to comply with the Modern Slavery Act 2015, KpH will both continue to monitor and mitigate any risks within KpH and our supply chain, so that effective controls and contingency plans can be put in place if required.

In 2021, we will commit to undertake, an annual audit of our labour-only Supplier's processes (regarding recruitment and payment) to ensure that they continue to satisfy legislation and our own Modern Slavery and Human Trafficking policies. These audits will be random and unannounced.

The success of this policy is dependent upon all employees, supply chains and subcontractors playing an important part in helping to detect and eradicate slavery. As such, all individuals are encouraged to report any suspected slavery to our "Speak Out" email, the details of which are at all our sites and offices as part of a poster and awareness campaign.

Training

To ensure a clear understanding of the Modern Slavery Act 2015 and the risks, we intend to roll out training to all relevant members of staff.

A specific Tool Box Talk has been created and will be delivered as part of our on-site training and development programme. Modern day slavery awareness training is provided for all new site Supervisors.

In our capacity as a member of the Supply Chain Sustainability School, we are able to download training videos modules on the Modern Slavery Act which will be made available to our supply chain and other partners, during the course of 2020-2021.

Summary

This statement is made pursuant to s.54(1) of the Modern Slavery Act 2015 and serves as our Modern Slavery and Human Trafficking statement for the financial year ending 2021. This statement will be reviewed annually.

Signed for KpH Group Limited:

Mr Kevin Potter Managing Director	
Date:	03/08/2021



Non English Speaking Personnel Policy Statement

This Policy sets out the ways in which KpH Deconstruction Services Ltd will seek to assist employees/sub-contractors on site who have difficulties understanding English, or employees who have low literacy levels.

There are a number of ways you can communicate with them to encourage their involvement. The aim is to achieve the same standard of understanding and involvement as for an English speaker.

KpH Deconstruction Services Ltd will commit to undertake one or more of the following which will ensure that the required assistance is given to involve and consult with such employees:

- Ensure adequate time to consult with employees where language and/or literacy may be issues so they can absorb the information and respond to you.
- Encourage employees to express their views in their preferred language by using interpreters.
- Ask a work colleague to interpret, although these employees may need training if they are asked to undertake this role.
- Get information translated and check that this has been done clearly and accurately by testing it with native speakers.
- Use pictorial information and internationally understood pictorial signs where appropriate.
- Where information has to be in English, use clear and simple materials, and allow more time.

KpH Deconstruction Services Ltd recognise that the key to individual consultation is to make sure that everybody is involved and will therefore take the necessary steps to ensure the methods adopted will reach all members of the workforce.

Signed for KpH Deconstruction Services Limited:

A handwritten signature in black ink, appearing to read 'K. J. Potter'.

Date: 3rd August 2021

Kevin Potter
Managing Director



On-Site Mobile Phones Policy

The use of mobile phones (Calls, Texting, Facebook and Twitter) and other electronic devices (e.g. Apple watch or similar) have been implicated in a number of accidents at work (e.g. being distracted whilst working at height or at ground level being unable to hear a warning or the approach of a vehicle or item of plant).

Company Policy (and Site Rules) requires the use of mobile phones or other electronic devices to be restricted to the canteen, rest area or designated compound areas and only during official breaks (other than the Site Manager as part of the Emergency Arrangements).


During induction all supervisors, workers and visitors (employees and subcontractors) must be made aware of this Policy and should be instructed to keep mobile phones and any other electronic devices switched off when they are in the work area.

The Policy should also be discussed with subcontractors at pre-order meetings to ensure everyone is aware of the arrangements prior to attending the site.

Exceptional circumstances would be reviewed on a case by case basis such as expectant fathers where phones would be held by a supervisor in the event the operative requires contacting, such cases must be advised to the Site Manager during signing in each day.

If, anyone is discovered using a mobile phone or any other electrical devices on site during working time it will be considered a breach of the Site Rules and Company Policy and will therefore be dealt with in accordance with the Company's Disciplinary Procedure.

Signed for KpH Group Limited:

Mr Kevin Potter Managing Director	
Date:	03/08/2021



Quality Policy Statement

The scope of the company is primarily involved with specialist services to the Construction and Petro-Chemical Industries. We undertake Demolition works, Soft Strip and Enabling, Fuel Tank Cleaning and Removal, Land Remediation & Groundwork and Plant/Machinery Removal & Replacement and their associated services.

The quality policy of the Company is to maintain and improve its reputation for providing a high quality of service. The aim of the Company is to market and provide services of a high standard that will merit and earn client satisfaction in our competitive market. The Company is committed to comply with all the quality standard requirements and will seek to continually improve the effectiveness of the "Quality Management System".

The Company holds regular quality review meetings that monitor and maintain the Company's Quality Policy and Procedures in relation to the project work we undertake and have completed. The policy is assessed to ensure that it is still relevant to the Company's scope and activities as well as our current contractual requirements. The Company will ensure that all its staff are fully aware of the Company's quality policy and their duties and responsibilities to it. All personnel will receive Quality Policy training and receive regular updates and information to ensure that they adhere and comply with the Company's stated quality aims and objectives.

The Company stresses the importance of a complete quality service to all company personnel. All personnel are involved in carrying out the Quality Policy. The sections of the Quality Manual, which are relevant to each person's work, will be reviewed regularly and amended and then discussed with the employees and then incorporated into the Quality Procedures. The Quality Controller as part of the Company's quality management system will record all of the document control amendments.

The Management of the Company is committed to a policy of Quality Assurance throughout the Company's activities, by specifically ensuring that the product quality satisfies the specific contractual obligations of all our customers and complies with the Standards of Quality specified in ISO 9001:2000 (ISO 14001:2015) and also the relevant Health and Safety requirements together with any other relevant legislation and Codes of Practice which may augment these standards.

The Quality Manual and the associated Quality Procedures are approved by the undersigned and are the authoritative documents relating to Quality within the Company.

Signed for KpH Group Limited:

Mr Kevin Potter Managing Director	
Date:	03/08/2021



RIGHT TO WORK IN THE UK

Checking Process and Checklist

CONTENTS

INTRODUCTION	2
RIGHT TO WORK PROCESS	3
1. Obtaining Acceptable Documents Showing Right To Work	3
2. Check the Validity of the Documents	4
3. Seek Further Advice If:	5
4. Take a Copy of the Documents Sign and Date Each Page Copied	5
5. Unsuccessful Candidates	6
6. Storage of Documents	6
EXAMPLE RIGHT TO WORK CHECKLIST FOR EMPLOYEE FILE	7

INTRODUCTION

It is illegal to employ someone who is not allowed to work in the UK. As an employer, you have a duty to check potential employees' documents, before you employ them, to ensure they have the right to work in the UK.

To ensure that you meet your obligations under the Immigration, Asylum and Nationality Act 2006, **Right to Work documentation must be presented before, or on the first day of service.** If documents are not presented before/on the first day of employment then the individual **must** be sent home to collect the documentation. Their employment cannot begin until your company has seen the original documentation which confirms their right to work.

How to Use this Document

Follow the process outlined below when you meet with a new employee before or on their first day of employment.

Use the checklist at the end of the document to ensure you have covered all the steps correctly. Detach the checklist and store it on the employee's personal file, along with signed and dated copies of documents that have been presented to you.

Summary: Conducting a Right to Work Check

There are 3 basic steps to conducting a right to work check:

1. Obtain original versions of one or more of the acceptable documents;
2. Check the documents in the presence of the holder of the documents; and
3. Make copies of the documents; retain the copies and a record of the date on which the check is made.

Each step in the right to work check process is addressed in detail below.

When completed correctly, this can provide a 'statutory excuse' against a civil penalty.

RIGHT TO WORK PROCESS

1. Obtaining Acceptable Documents Showing Right To Work

- You must be provided with one of the documents or combinations of documents in List A or List B below as proof that someone is allowed to work in the UK.
- You must only accept original documents.

LIST A

Documents to Establish a Continuous Statutory Excuse	
1.	A passport showing the holder, or a person named in the passport as the child of the holder, is a British citizen or a citizen of the UK and colonies having the right of abode in the UK
2.	A passport or national identity card showing that the holder, or a person named in the passport as the child of the holder, is a national of a European Economic Area country or Switzerland
3.	A Registration Certificate or Document Certifying Permanent Residence issued by the Home Office, the Border and Immigration Agency, or the UK Border Agency ¹ to a national of a European Economic Area country or Switzerland
4.	A Permanent Residence card or document issued by the Home Office, the Border and Immigration Agency, or the UK Border Agency to the family member of a national of a European Economic Area country or Switzerland
5.	A current Biometric Immigration Document (Biometric Residence Permit) issued by the Home Office to the holder which indicates that the person named in it is allowed to stay indefinitely in the UK, or has no time limit on their stay in the UK
6.	A current passport endorsed to show that the holder is exempt from immigration control, is allowed to stay indefinitely in the UK, has the right of abode in the UK, or has no time limit on their stay in the UK
7.	A current Immigration Status Document issued by the Home Office, the Border and Immigration Agency, or the UK Border Agency to the holder with an endorsement indicating that the person named in it is allowed to stay indefinitely in the UK or has no time limit on their stay in the UK, together with an official document giving the person's National Insurance number and their name by a Government agency or a previous employer (a P45, P46, National Insurance card, or letter from a Government agency)
8.	A full birth or adoption certificate issued in the UK which includes the name(s) of at least one of the holder's parents together with an official document issued by a previous employer or Government agency with the person's name and National Insurance number (a P45, P46, National Insurance card, or letter from a Government agency)
9.	A birth or adoption certificate issued in the Channel Islands, the Isle of Man or Ireland together with an official document issued by a previous employer or Government agency with the person's name and National Insurance number (a P45, P46, National Insurance card, or letter from a Government agency)
10.	A certificate of registration or naturalisation as a British citizen together with an official document issued by a previous employer or Government agency with the person's name and National Insurance number (a P45, P46, National Insurance card, or letter from a Government agency)

¹ The UK Border Agency (UKBA) has been replaced by UK Visas and Immigration (UKVI) and the Border Force

List B

Seek further advice if List B documents are supplied.

A current passport must be provided, in addition to one of the documents listed below.

GROUP 1: Documents where a time-limited statutory excuse lasts until the expiry date of leave.	
1.	A current passport endorsed to show that the holder is allowed to stay in the UK and is allowed to do the type of work in question (this must be supplied in addition to one of the documents below)
2.	A current Biometric Immigration Document (Biometric Residence Permit) issued by the Home Office to the holder which indicates that the person named in it can stay in the UK and is allowed to do the type of work in question
3.	A current Residence Card (including an Accession Residence Card or a Derivative Residence Card) issued by the Home Office, the Border and Immigration Agency, or the UK Border Agency to a non-European Economic Area national who is a family member of a national of a European Economic Area country or Switzerland or who has a derivative right of residence
4.	A current Immigration Status Document containing a photograph issued by the Home Office to the holder with a valid endorsement indicating that the named person may stay in the UK, and is allowed to do the type of work in question, together with an official document issued by a previous employer or Government agency with the person's name and National Insurance number (a P45, P46, National Insurance card, or letter from a Government agency)
GROUP 2: Documents where a time-limited statutory excuse lasts for 6 months.	
1.	A Certificate of Application issued by the Home Office under regulation 17(3) or 18(2) of the Immigration (European Economic Area) Regulations 2006 to a family member of a national of a European Economic Area country or Switzerland stating the holder is permitted to take employment which is less than 6 months old together with a Positive Verification Letter from the Home Office Employer Checking Service
2.	An Application Registration Card (ARC) issued by the Home Office, the Border and Immigration Agency stating that the holder is 'ALLOWED TO WORK' or 'EMPLOYMENT PERMITTED' together with a Positive Verification Letter from the Home Office Employer Checking Service
3.	A Positive Verification Notice issued by the Home Office Employer Checking Service to the employer or prospective employer which indicates that the named person may stay in the UK and is permitted to do the work in question

2. Check the Validity of the Documents

- You must satisfy yourself that the documents are genuine and that the person presenting the documents is the prospective employee, the rightful holder and allowed to do the type of work you are offering.
 1. Are photographs consistent with the appearance of the person and consistent across documents (where applicable)?
 2. Are the dates of birth listed consistent both across documents and with the appearance of the person?
 3. Are expiry dates for limited leave to enter or remain in the UK in the future i.e. they have not passed?

4. Do the endorsements (stamps, visas etc.) show the person is able to do the type of work you are offering (e.g. there are no restrictions – see below)?
5. Are you satisfied that the documents are genuine, have not been tampered with and belong to the holder?
6. Have you asked for further documents to explain why you have been given documents with different names (e.g. marriage certificate/divorce decree/deed poll)?

NOTE: Restrictions

If documents show a restriction on the type of work they can do and/or the hours they can work, make sure the job you give them does not break those conditions.

International students who have a limited right to work are required to provide an employer with evidence of their academic term and vacation times for the duration of their studies in the UK while they work.

If there are any queries or concerns relating to the documents provided, use the Home Office Employer Checking Service: <https://www.gov.uk/legal-right-work-uk> or ECS Checking Form.

3. Seek Further Advice If:

The individual is non-EU/EEA or Swiss.

The individual has supplied List B documents (indicating that they have limited right to work in the UK).

The Individual is a Croatian national.

The individual has an outstanding application or appeal to vary or extend their leave in the UK.

Advice can be obtained from:

<https://www.gov.uk/check-job-applicant-right-to-work>

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/426972/frequently_asked_Qs_illegal_working_civil_penalty_May_final.pdf

4. Take a Copy of the Documents Sign and Date Each Page Copied

Copies should be taken in full, and in a format that cannot be altered. Sign and date each page copied.

If a passport has been provided ensure the following are copied:

- Pages providing the holder's personal details; nationality; photo; date of birth; signature; date of expiry and biometric details or other documents as appropriate.
- Any pages containing UK Government endorsements' showing the person is allowed to work in the UK and carry out the work you are offering (if applicable).

Ensure both sides of a Biometric Residence Permit are copied (if applicable).

Ensure letters from the Home Office/ UK Border Agency/ UK Visas & Immigration regarding right to work in the UK are copied (if applicable).

Supporting documents (e.g. marriage certificate/divorce decree/deed poll) to prove a change of name or personal details should also be copied (if applicable).

5. Unsuccessful Candidates

Where documents are copied at interview stage, documents for unsuccessful candidates must be securely shredded once the candidate has been notified that their application was not successful. Notification should be given to the candidate that this documentation has been destroyed.

6. Storage of Documents

Copies of documents for the successful candidate/new employee must be stored on a personal file. **A right to work document checklist has been included on page 6.**

These must be kept for two years after the employee has left your employment.

General Notes:

EEA Nationals Who Can Live and Work Without Restriction EEA Countries are: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.

You should require any person who claims to be an EEA national to produce an official document showing their nationality. This will usually be either a national passport or national identity card which indicates that the holder is a national of an EEA state.

Registration Certificates: some EEA nationals may also have been issued with a registration certificate to confirm that they are living in the UK in compliance with the EEA Regulations, either by fulfilling the requirements for residence (also known as 'exercising Treaty rights') or by residing in the UK as the family member of another EEA national who is exercising Treaty rights.

Document Certifying Permanent Residence: some EEA nationals may be able to produce a document certifying that they have a right of permanent residence in the UK. Under EU law, an EEA national can acquire permanent residence after five years' lawful and continuous residence in the UK.

All of these documents (passport establishing EEA nationality, identity card establishing EEA nationality, registration certificate and document certifying permanent residence) are included in List A of acceptable documents, and production of any one of them will provide you with a continuous statutory excuse if checked and copied correctly before the person starts working for you.

Croatian Nationals:

Since 1 July 2013, as EU nationals, Croatians are able to move and reside freely in any EEA Member State. However, a Croatian national who wishes to work in the UK and who is subject to the worker authorisation requirement will need to obtain an accession worker authorisation document (permission to work) before starting any employment.

EXAMPLE RIGHT TO WORK CHECKLIST FOR EMPLOYEE FILE

Name:	
Role and Department:	
Date:	

Right to Work in UK Confirmed: Yes No Restricted

STEP 1	
Original document seen (e.g. Passport)	
Document listed on List A or List B?	
Date leave/right to work expires (if applicable).	
STEP 2	
Checked validity of documents (in the presence of the holder) using criteria in Step 2.	
STEP 3	
Copy of relevant pages taken. Each page has been signed and dated by the individual checking the documents.	
STEP 4 Where List B Documents Provided	
Further advice sought where List B documents provided.	
Re-check List B documents on 1 April each year and on the expiry date of leave.	
STEP 5 If applicable	
Any copies of documentation from unsuccessful candidates destroyed.	
STEP 6	
Signed and dated copies of documents stored on employee personal file.	
Signed by Manager Responsible for check:	

Reviewed: 3rd August 2021

Next Review By: 2nd August 2022



SOCIAL MEDIA POLICY

1. Introduction

- 1.1 This Social Media Policy applies to all employees, contractors and agents of KpH Group Ltd (“the Company”) who use computers, mobile devices, networks and other communications equipment and systems provided by the Company (“Users”).
- 1.2 This Social Media Policy exists to address the use by Users of all types of social network and social media platforms including, but not limited to, Facebook, Twitter, LinkedIn, Google+, Pinterest, Tumblr and Instagram (collectively, “Social Media”).
- 1.3 The purpose of this Social Media Policy is to minimise the various risks to the Company presented by Social Media usage.
- 1.4 No part of this Social Media Policy shall be deemed to form a part of any employee’s contract of employment. It may be amended by the Company at any time and for any reason.

2. General Principles

There are certain general principles that all Users should keep in mind when using Social Media whether for personal use or for authorised work-related purposes. The Company expects all Users to:

- 2.1 Use Social Media responsibly and professionally, and at all times in accordance with their duties.
- 2.2 Be mindful of what constitutes confidential, restricted or other proprietary information and ensure that such information is never disseminated over Social Media without the expressed consent of a Division Manager at KpH Group Ltd.
- 2.3 Ensure that their use of Social Media does not breach any other of the Company’s policies including, but not limited to, its Information Security Policy; Equal Opportunities and Diversity Policy; Disciplinary Policy and Procedure and Data Protection Policy.
- 2.4 Ensure that their use of Social Media does not breach any other laws, regulatory requirements, or other applicable rules set out by regulatory bodies and other organisations.
- 2.5 Ensure that they do not breach any copyright or other intellectual property rights when using Social Media.
- 2.6 Be mindful of the fact that any communication may be relied upon in court, to the advantage or detriment of the individual or the Company and conduct their use of Social Media accordingly.

3. Personal Social Media Use

Users may use Social Media for personal purposes occasionally during work hours [for example, during breaks] provided that such usage complies with the provisions of this Social Media Policy and provided that it does not interfere with their work responsibilities or productivity.

Business Social Media Use

- 3.1 Certain Users may from time to time be required to use Social Media on behalf of the Company. A User should only use Social Media on behalf of the Company with the authorisation of the Division Manager.
- 3.2 Use of Social Media for business purposes must comply with the provisions of this Social Media Policy at all times.
- 3.3 Users using Social Media on behalf of the Company may from time to time be required to interact with other internet users via Social Media, for example, in response to posts or enquiries regarding the Company. Unless the instructions issued to that User (see paragraph 4.1) specifically authorise the User to respond without further approval, the User may not respond to any such communications without the prior approval of their Division Manager. In any event, no User using Social Media on behalf of the Company should respond to such communications, with or without prior approval, without first consulting the relevant individual and/or department unless they are fully knowledgeable of the relevant topic and suitably qualified to respond.
- 3.4 Before using Social Media on behalf of the Company, Users may require training in order to do so, or may be required to demonstrate that they have already received suitable training, either from the Company or from a previous employer or other organisation.

4. Acceptable Use of Social Media

- 4.1 Unless specifically instructed to do so by their Division Manager, Users should make it clear that they are posting on Social Media as themselves, not as the Company, and that all views expressed on Social Media by that User are the author's own and do not necessarily reflect the views of the Company.
- 4.2 Unless using Social Media on behalf of the Company, Users should not use any Social Media accounts belonging to, or otherwise associated with, the Company.
- 4.3 Company email addresses may only be used to sign up to Social Media websites for work-related purposes. Users should be aware that their Company email address will cease to function should they cease to work for or with the Company and may result in the Social Media account(s) in question being inaccessible.
- 4.4 Users should always be respectful to others when using Social Media and should always be mindful of the fact that their association with the Company may be known to anyone at any time. The conduct of all Users on Social Media may reflect on the Company, whether positive or negative. This applies whether a User is using Social Media for business purposes or for personal purposes, whether during work hours or otherwise.
- 4.5 If a User is unsure as to the appropriateness of a post or any other Social Media activity with respect to this Social Media Policy, they should consult their Division Manager before continuing.

5. Unacceptable and Prohibited Use of Social Media

- 5.1 Users must not use Social Media to defame or otherwise disparage the Company or any of its employees, contractors, agents, or other affiliated third parties and organisations.
- 5.2 Users must ensure that their use of Social Media does not damage the Company, its interests, or its reputation, whether directly or indirectly, in any way.
- 5.3 As under paragraph 5.1, unless specifically instructed to do so, Users must not represent themselves on Social Media as the Company or as posting on behalf of the Company.

- 5.4 Users may not share confidential, commercially sensitive or other proprietary business information belonging to the Company or any of its employees, contractors, agents, or other affiliated third parties and organisations on Social Media unless specifically authorised to do so by their Division Manager.
- 5.5 Users may not use any intellectual property belonging to the Company on Social Media (including, but not limited to, trademarks and logos) unless specifically authorised to do so by their Division Manager.
- 5.6 Users may not add contacts made during the course of their duties to their personal Social Media accounts without the authorisation of their Division Manager.

6. Monitoring

- 6.1 The Company may monitor Users' communications and internet usage (including, but not limited to Social Media) for the following reasons:
 - 6.1.1 To ensure that Company policies and guidelines are followed, and that standards of service are maintained.
 - 6.1.2 To provide evidence of transactions and communications.
 - 6.1.3 To help combat unauthorised use of the Company's computers, mobile devices, networks and other communications equipment and systems and to maintain security.
 - 6.1.4 If the Company has reason to believe that a User has been viewing or sending offensive or illegal material (including, but not limited to that which breaches another party's intellectual property rights).
 - 6.1.5 If the company has reason to believe that a User has been spending an unreasonable amount of time viewing non-work-related sites (including, but not limited to, Social Media) and/or sending and receiving an unreasonable number of personal communications.
 - 6.1.6 In order to better understand the requirements of the Company in terms of the provision of computers, mobile devices, networks and other communications equipment and systems.
- 6.2 Users should be aware that all internet and email traffic data sent and received using the Company's communication systems is logged, including websites visited, times of visits, and duration of visits. Any personal use of the internet, including but not limited to Social Media, will therefore be logged also, irrespective of whether or not it is in compliance with this Social Media Policy and other Company policies. Users who wish to avoid the possibility of the Company becoming aware of any political or religious beliefs or affiliations that they would prefer to keep private should avoid visiting websites that might reveal such information. By using the Company's computers, mobile devices, networks and other communications equipment and systems, Users are taken to consent to their personal internet use and communications being logged and monitored by the Company. The Company shall ensure that any monitoring under this Social Media Policy complies fully with all applicable laws including, but not limited to, the Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000, and the Human Rights Act 1998.
- 6.3 When monitoring emails, the Company will normally restrict itself to looking at the address and email headers. If, however, it is considered necessary, the Company may open and read emails. Users should be aware that sensitive and confidential communications should not be sent by email because it cannot be guaranteed to be private.

7. Recruitment


The Company may use internet searches to carry out due diligence as part of its recruitment process. In these circumstances, the Company will act in accordance with its equal opportunities and data protection obligations.

8. Misuse and Compliance

- 8.1 Any User found to be in breach of this Social Media Policy will be treated in line with the KpH disciplinary procedure.
- 8.2 The viewing, transmission, downloading, uploading or accessing in any way, whether through Social Media or otherwise, of any of the following material using the Company's computers, mobile devices, networks or other communications equipment and systems will amount to gross misconduct with the possibility of summary dismissal:
- 8.2.1 Material which is pornographic, sexist, racist, homophobic, paedophilic, or any other discriminatory or otherwise obscene or offensive material.
 - 8.2.2 Illegal or criminal material, including material which breaches copyright or any other intellectual property right.
 - 8.2.3 Any material which has the object or effect of causing harassment to the recipient.
 - 8.2.4 Material which the User knows, or ought to know, is confidential, restricted or otherwise proprietary information and which they are not authorised to deal with.
 - 8.2.5 Any website (Social Media or otherwise) which the Company has blocked access to.
- 8.3 Any questions regarding this Social Media Policy should be referred to a Division Manager.
- 8.4 If any User becomes aware of any content on Social Media that reflects poorly on the Company or otherwise defames or disparages the Company, they should contact the Division Manager.

This policy has been approved and authorised by:

On behalf of KpH Group Limited

Mr Kevin Potter Managing Director	
Date:	03/08/2021



STAFF WELL-BEING POLICY

CONTENTS

1.	Introduction	2
2.	Statement of Intent	2
3.	Responsibilities for Implementing the Staff Well-Being Policy	2
4.	Arrangements for Well-Being and Stress Prevention	3
5.	Communicating the Well-Being Policy	3

1. Introduction

KpH Group Ltd as an employer has a duty to ensure the health, safety and welfare of its employees as far as reasonably practicable. It is also required to have in place measures to mitigate as far as practicable factors that could harm employees' physical and mental well-being, which includes work related stress. This duty extends only to those factors which are work-related and within the Company's control.

The Health and Safety Executive's definition of work-related stress is "the adverse reaction a person has to excessive pressure or other types of demand placed on them" We recognise that there is an important distinction between "reasonable pressures" which stimulate and motivate and "stress" where an individual feels they are unable to cope with excessive pressures or demands placed upon them.

The Health and Safety Executive have produced a number of Management Standards which cover the primary sources of stress at work that, if not properly managed, are associated with poor health and well-being, lower productivity and increased sickness absence. These are:

Demands	i.e. workload, work patterns and the work environment
Control	i.e. how much say the person has in the way they do their work
Support	i.e. the encouragement, sponsorship and resources provided by the organisation, line management and colleagues
Relationships	i.e. promoting positive working to avoid conflict and dealing with unacceptable behaviour
Role	Such as whether people understand their role within the organisation and whether the organisation ensures that they do not have conflicting roles.
Change	Such as how organisational change (large or small) is managed and communicated within the organisation.

2. Statement of Intent

The Managing Director acknowledges the potential impact that work has on an individual's physical and mental health and that there is a moral and legal duty to take steps to promote employee well-being as far as reasonably practicable.

The organisation is committed to fostering a culture of co-operation, trust and mutual respect, where all individuals are treated with dignity and can work at their optimum level.

It recognises that work related stress has a negative impact on employees well-being and that it can take many forms so therefore needs to be carefully analysed and addressed at an organisational level.

3. Responsibilities for Implementing the Staff Well-Being Policy

The Director and Senior Managers will:

- support steps taken to develop a culture of co-operation, trust and mutual respect;
- champion good management practices;
- encourage initiatives and events that promote health and well-being.

Managers and Supervisors will:

- Treat individuals reporting to them with consideration and dignity and promote a culture of mutual respect in the teams they manage.
- Ensure that there is good communication within their team and there are opportunities for individuals to raise concerns about their work.
- Encourage their staff to participate in events and initiatives which promote well-being and more effective working.
- Take action in the interests of all their colleagues where performance by a member of staff may cause stress to their colleagues.

Employees will:

- Treat colleagues and all other persons with whom they interact during the course of their work with consideration, respect and dignity.
- Raise concerns with their line manager if they feel there are work issues that are causing them stress and having a negative impact on their well-being.
- Take responsibility for their own health and well-being by adopting healthy lifestyles.
- Take responsibility for their own development skills as one of the means to enable them to work effectively in their team and so reduce the risk of stress.
- Take responsibility for working effectively in their assigned roles, thus helping to avoid causing stress to their colleagues.

4. Arrangements for Well-Being and Stress Prevention

These include the following:

- recruitment and selection procedures;
- clear job descriptions and person specifications to ensure that the 'right' person is recruited for the job.
- training and Development procedures to ensure that individuals have the necessary skills and competencies to undertake the tasks/duties required of them;
- promotion and reward procedures;
- suitable adaptations for disability;
- harassment and anti-bullying procedures.

5. Communicating the Well-Being Policy

The Well-Being Policy will be brought to all new employees' attention at Company Induction and will be available for reference at the Company Head Office at all times.

The contents of the policy will be covered during site inductions and specific tool box talks.



Sustainable Timber Procurement Policy Statement

We, KpH Group, recognise that:


- Forests are essential for human survival and well-being. They are among the most biodiverse and valuable terrestrial ecosystems on the planet. They provide us with food, oxygen, shelter, recreation, and spiritual sustenance; and they contribute to the livelihoods of 1.6 billion people worldwide. The biodiversity of forests, the variety of genes, species, and forest ecosystems underpins these goods and services, and is the basis for long-term forest health and stability.
- Promoting ways to use forest biodiversity in a sustainable way, and with clear social and economic benefits for the poor, is important.
- Forest certification provides evidence of sustainable forest management, yet at present, less than 10% of the world's forests are certified. Mainstreaming forest certification systems (such as PEFC and FSC) will assist in promoting sustainable forest management.

As a user of timber and wood-based products, KpH Group, recognizes that it has a responsibility to current and future generations and will therefore strive to promote sustainable forest management. By demanding products from sustainably managed forests, we aim to stimulate the improvement of forest management and discourage unsustainable management practices.

We, KpH Group, will give preference to suppliers who can demonstrate that their products originate from sustainably managed forests. We consider it important that the origin of our wood-based products can be demonstrated through credible, independent Chain of Custody certification based on international standards and norms.

In this context, we recognize credible third-party certification systems accepted by government procurement policies and guidelines, such as the UK Central Point of Expertise of Timber or the EU Green Public Procurement criteria, as evidence of responsible and sustainable sourcing. This includes the Programme for the Endorsement of Forest Certification (PEFC) and the Forest Stewardship Council (FSC), the two largest forest certification systems globally.

Signed for KpH Group Limited:

Mr Kevin Potter Managing Director	
Date:	03/08/2021



Whistle-Blowing Policy

1. ADVICE AND INSTRUCTIONS FOR STAFF

The term "whistle-blowing" has no legal definition within UK law; however, it has been used to describe incidents where an employee publicly discloses some alleged wrongdoing within an organisation.

The Public Interest Disclosure Act 1998 aims to promote greater openness in the workplace and, by amending the Employment Protection Act 1996, protects "whistle-blowers" from detrimental treatment, i.e. victimisation or dismissal, for raising concerns about matters in the public interest. In providing this protection, the Act also reinforces the obligations of all persons employed by the Company not to disclose to external sources any trade secrets or confidential information acquired during the course of their employment unless they fall within the qualifying for protection disclosures.

This statement sets out the Company's Policy and provides in some detail advice and guidance to staff on the scope of the Policy. It explains that any member of staff who has a reasonable belief that there is serious malpractice relating to any of the protected matters specified in the Policy may raise a concern under the procedure agreed by the Board and which is described in this statement. There is also information about the rights of staff to raise the matter externally if they are not satisfied with the Company's response and the protection afforded to them if they choose to do this after the internal procedures have been exhausted.

2. WHISTLE-BLOWING POLICY

- Introduction
- Scope of the Policy
- Who Can Raise a Concern?
- Procedure
- Process
- Investigation
- Records
- Reporting of Outcomes
- Advice for Staff Raising a Concern
- Complaints of Retaliation as a Result of Disclosure
- External Disclosure

1.1. Introduction

All persons employed by the Company are under an obligation implied in their contract of employment to give honest and faithful service to their employer. This includes an obligation not to disclose to external sources any trade secrets or confidential information acquired during the course of employment or act in a manner that will undermine the mutual trust and confidence on which the employment relationship is based. The Public Interest Disclosure Act 1998 complements those obligations by providing protection to employees for disclosure made without malice and in good faith of certain specific confidential information to a third party in defined circumstances. These are outlined below in paragraph 3. The purpose of this policy is to provide a means by which employees are enabled to raise concerns with the appropriate authorities if they have reasonable grounds for believing there is serious malpractice within the Company. The Company encourages staff to raise matters of concern responsibly through the procedures laid down in this policy statement.

1.2. Scope of the Policy

The policy is designed to deal with concerns raised in relation to the specific issues which are in the public interest and are detailed in paragraph 3 below, and which fall outside the scope of other Group policies and procedures. The policy will not apply to personal grievances concerning an individual's terms and conditions of employment, or other aspects of the working relationship, complaints of bullying or harassment, or disciplinary matters. Such complaints will be dealt with under existing procedures on grievance, bullying and harassment, discipline and misconduct in research. Details of these procedures will be found in the relevant staff handbook. They are also published on the intranet.

The policy may deal with specific concerns which are in the public interest and may include:

- a criminal offence;
- failure to comply with legal obligations or with the Statutes, Ordinances and Regulations of the Company;
- financial or non-financial misadministration or malpractice or impropriety or fraud;
- professional malpractice;
- a risk to the health or safety of any individual;
- environmental damage;
- a miscarriage of justice;
- improper conduct or unethical behaviour;
- attempts to suppress or conceal any information relating to any of the above.

If in the course of investigation any concern raised in relation to the above matters appears to the investigator to relate more appropriately to grievance, bullying or harassment, or discipline, those procedures will be invoked.

1.3. Who Can Raise a Concern?

Any member of staff who has a reasonable belief that there is serious malpractice relating to any of the protected matters specified in paragraph 3 above may raise a concern under the procedure detailed in paragraph 6 below. The issues raised under the protected list may relate to another member of staff, a group of staff, the individual's own branch/ department or another part of the Company. Concerns must be raised without malice and in good faith, and the individual must reasonably believe that the information disclosed, and any allegations contained in it, are substantially true. The disclosure must not be made for purposes of personal gain, and in all the circumstances it must be reasonable to make the disclosure. The Company will ensure that any member of staff who makes a disclosure in such circumstances will not be penalised or suffer any adverse treatment for doing so. However, a member of staff who does not act in good faith or makes an allegation without having reasonable grounds for believing it to be substantially true, or makes it for the purposes of personal gain, or makes it maliciously or vexatiously may be subject to disciplinary proceedings.

In view of the protection afforded to a member of staff raising a bona fide concern, it is preferable if that individual puts his/her name to any disclosure. The identity of the person raising the matter will be kept confidential, if so requested, for as long as possible, provided that this is compatible with a proper investigation. Anonymous complaints are not covered by this procedure, but may be reported, investigated or acted upon as the person receiving the complaint sees fit (including the use of this procedure), having regard to the seriousness of the issue raised, the credibility of the complaint, the prospects of being able to investigate the matter, and fairness to any individual mentioned in the complaint.

1.4. Procedure

Initial Step

Normally any disclosure about a protected matter should be made in the first instance to:

- Kevin Potter (Managing Director)

If the disclosure is about the Managing Director, the member of staff may raise the concern directly with Lyndsey West (Division Manager).

The person to whom the disclosure is made will decide whether the matter should be dealt with under this procedure. If he or she considers that the matter should be dealt with under a different Company procedure, s/he will advise the person making the disclosure as to the appropriate steps which should be taken.

1.5. Process

The person to whom the disclosure is made will normally consider the information and decide whether there is a prima facie case to answer. He or she will decide whether an investigation should be conducted and what form it should take. This will depend on the nature of the matter raised and may be:

- investigated internally;
- referred to the External Auditors;
- the subject of independent enquiry.

Some matters following investigation, will need to be referred to the relevant outside body, e.g. the Police. If the person to whom the disclosure is made decides not to proceed with an investigation, the decision will be explained as fully as possible to the individual who raised the concern. It is then open to the individual to make the disclosure again either to another of the persons specified in the paragraph above or to the Chair of the Audit Committee.

1.6. Investigation

Any investigation will be conducted as sensitively and speedily as possible. The employee will be notified of the intended timetable for the investigation. The person to whom the disclosure is made may authorise an initial investigation to establish the relevant facts. The investigation may be conducted by the internal auditor in the case of a financial irregularity, or by another person. The investigator will report his or her findings to the person to whom the disclosure was made, who will then decide if there is a case to answer and what procedure to follow. This may include taking steps with the competent authority to set up a special internal independent investigation or reference to some external authority, such as the police, for further investigation. The decision may be that the matter would be more appropriately handled under existing procedures for grievance, bullying and harassment, or discipline.

Where disclosure is made the person or persons against whom it is made will be informed at an early stage of it and of the evidence supporting it, and they will be allowed to respond.

The individual making the disclosure will be informed of what action is to be taken.

Should an investigation or referral lead the appropriate Company authority to conclude there has been a breach of Company discipline, the member or members of staff responsible may, in addition to any civil or criminal proceedings, be subject to disciplinary action in accordance with the appropriate disciplinary procedures for the relevant category of staff.

1.7. Records

An official written record will be kept of each stage of the procedure (see also paragraph 10 below).

1.8. Reporting of Outcomes

A report of all disclosures and subsequent actions taken will be made by the persons deciding on the issues. This record should be signed and dated by the Investigating Officer and the person who made the disclosure. Where appropriate the formal record need not identify the person making the disclosure, but in such a case that person will be required to sign a document confirming that the complaint has been investigated. Such reports will normally be retained for at least five years. In all cases a report of the outcome will be made to the Chairman who will refer the report onwards appropriately if necessary.

1.9. Advice for Staff Raising a Concern

The Company acknowledges the difficult choice a member of staff may have to make in raising a concern. As the issues that prompt the concern are likely to be complex, how the member of staff proceeds with his or her concern will vary from situation to situation. The following advice is recommended if a member of staff wishes to make a disclosure:

- make any objections to illegal, unsafe or unethical practices promptly so as to avoid any misinterpretation of the motives for doing so;
- focus on the issues and proceed in a tactful manner to avoid unnecessary personal antagonism which might distract attention from solving the problem;

- be accurate in his/her observations and claims and keep formal records documenting relevant events.

Members of staff may also wish to seek independent legal advice.

1.10. Complaints of Retaliation as a Result of Disclosure

The Company accepts that it has an obligation to ensure that staff who make a disclosure without malice and in good faith are protected, regardless of whether or not the concern raised is upheld. A member of staff who has made a disclosure and who feels that, as a result, he or she has suffered adverse treatment should submit a formal complaint under the grievance procedure as set out in the relevant staff handbook and in the statutes and ordinances detailing what has been done to him or her. If it appears that there are reasonable grounds for making the complaint, the onus will be on the person against whom the complaint of adverse treatment has been made to show that the actions complained of were not taken in retaliation for the disclosure.

Where it is determined that there is a prima facie case that a member of staff has suffered adverse treatment, harassment or victimisation as a result of his or her disclosure, a further investigation may take place and disciplinary action may be taken against the perpetrator in accordance with the relevant procedure.

1.11. External Disclosure

If, having exhausted this procedure, a member of staff is not satisfied with the Company's response and reasonably believes that the information disclosed, and any allegation contained in it, are substantially true, he or she is at liberty to take the matter further by raising it with certain bodies or persons such as:

- a Member of Parliament;
- a Legal Adviser;
- other bodies or persons (if any) prescribed by the Secretary of State under Section 43F of the Employment Protection Act 1996, as amended by Section 1 of the Public Interest Disclosure Act 1998.

A member of staff who makes an external complaint in good faith to any prescribed body or person after exhausting the Company's procedure will be protected against victimisation or unfavourable treatment.

Signed for KpH Group Limited:

Mr Kevin Potter Managing Director	
Date:	03/08/2021



Work Safe Policy Statement

KpH Group Ltd acknowledge our responsibility under the Health and Safety at Work Act and associated regulations and recognise our duty of care and undertake to maintain safe systems affecting the health, safety and welfare of our employees. We will ensure that no one under our control is exposed to unacceptable levels of health or safety risks at work.

KpH Group Ltd operates a Work Safe Policy (or Right to Refuse to Work Policy) to protect our employees and ensure others not in our employment are not placed at risk.


Every member of KpH Group and every member of any Sub-Contractors team working on any KpH Group managed project(s), has the absolute right to decline to carry out work if they feel it is not safe to do so.

Where the operation of a machine, a site condition or a method of working constitutes a danger to the employee or another person the employee may refuse to work.

Any situation arising which leads to an individual refusing to work for Health and Safety reasons must be reported to the senior person on site as soon as possible, and no employee should continue to work until the working environment is made safe. The Health and Safety Manager should be informed. Escalation for resolving a Refusal to Work is through the Operations Manager or the Managing Director and their decision will be final.

Managers and staff are also encouraged to report any unsafe acts or conditions, which they have witnessed through the Near Miss Reporting procedure.

KpH Group Ltd will not discipline, discharge, suspend, lay off or demote an employee or impose any financial or other penalty on an employee who invokes the Refusal to Work Procedure.

Signed:		Position:	Managing Director
Name:	Kevin Potter	Date:	03/08/2021



Tight Fitting RPE User Facial Hair Policy

Compatibility and Suitability of RPE

As an employee using any PPE / RPE you will have received training and instruction in how to use your RPE device(s) correctly. You may also have received this information as a contractor.

You will have been Fit Tested with your device(s) which will have been chosen in consultation with you to define the most comfortable and compatible device for you. This will ensure you are able to wear it correctly.

As part of this process you have been given information and instruction in:

- How it works.
- How it should be worn.
- How it should be used, maintained, cleaned and stored.
- You will have been trained how to complete a robust pre-use fit check.
- You are provided with storage and a means of cleaning the device.
- For re-usable devices you are required to maintain your RPE and complete a monthly maintenance sheet and change filters.

As part of the training it will have been explained to you why it is vital that you remain clean shaven in the seal area of your tight-fitting respirator where it contacts and seals on your skin.

You will understand that the organisation requires that you are clean shaven within the previous 8 hour period prior to the work shift (for those working up to 8 hours) Or for those working more than 8 hours you should ensure a clean shaven state in the seal area within the 16 hours prior to you completing the shift.

Compliance

As you are aware compliance in this regard is a matter of Health and Safety and you have a duty to comply with these reasonable requests as part of this duty under the Health and Safety at work Act 1974 Section 7b ... to co-operate with him (the employer) so far as is necessary to enable that duty or requirement to be performed or complied with.

It is therefore our expectation that you as a competent trained and conscientious employee will help us to meet our duties under the Act and consistently adhere to this requirement.

Consultation

As part of our duty to consult with you we require you to work with us in this respect and raise any concerns or difficulties for you in this regard in the first instance through your line manager.

Disciplinary Procedure

As part of our duty to ensure we do not expose you to substances hazardous to health we will need to audit compliance in this area.

This may be on a formal or informal basis. If it is suspected by any supervisor, manager or a representative of the relevant competent authority that you may have breached this requirement we will reserve the right to implement sanctions or disciplinary measures to protect your health and our compliance with best practice.

Due to the serious nature of the consequences of exposure to respirable hazards we will not be able to allow you to work for/with us if you are not willing or able to comply in this area.

Alternatives to tight fitting RPE

It will have been explained to you the alternatives available to you if you are required to keep facial hair for these reasons.

- Health condition(s) that determine your inability to remain clean shaven in the seal area of the respirator.
- Religious practice that according to your faith and your particular standing/branch/movement/sect you are required to wear facial hair that may interfere with the seal of your respirator.

It is therefore your duty to inform us and work with us to help you to remain protected from airborne hazards not otherwise controlled, by consulting with us if this includes you.

The reasons above will not be automatically accepted without further clarification of the legitimacy of these reasons on an individual basis.

If you claim to meet the criteria for consideration for alternatives to tight fitting RPE we reserve the right to seek advice, confirmation / clarification from your medical advisors or specific religious institution you are part of.

The alternatives may include:

- Non-tight fitting RPE (Powered Air Purifying Respirators): These can be relatively expensive, and we will make decisions regarding this alternative based on reasonably practicable criteria.
- Where reasonably practicable being restricted from entering areas when there could be exposure to airborne hazards.

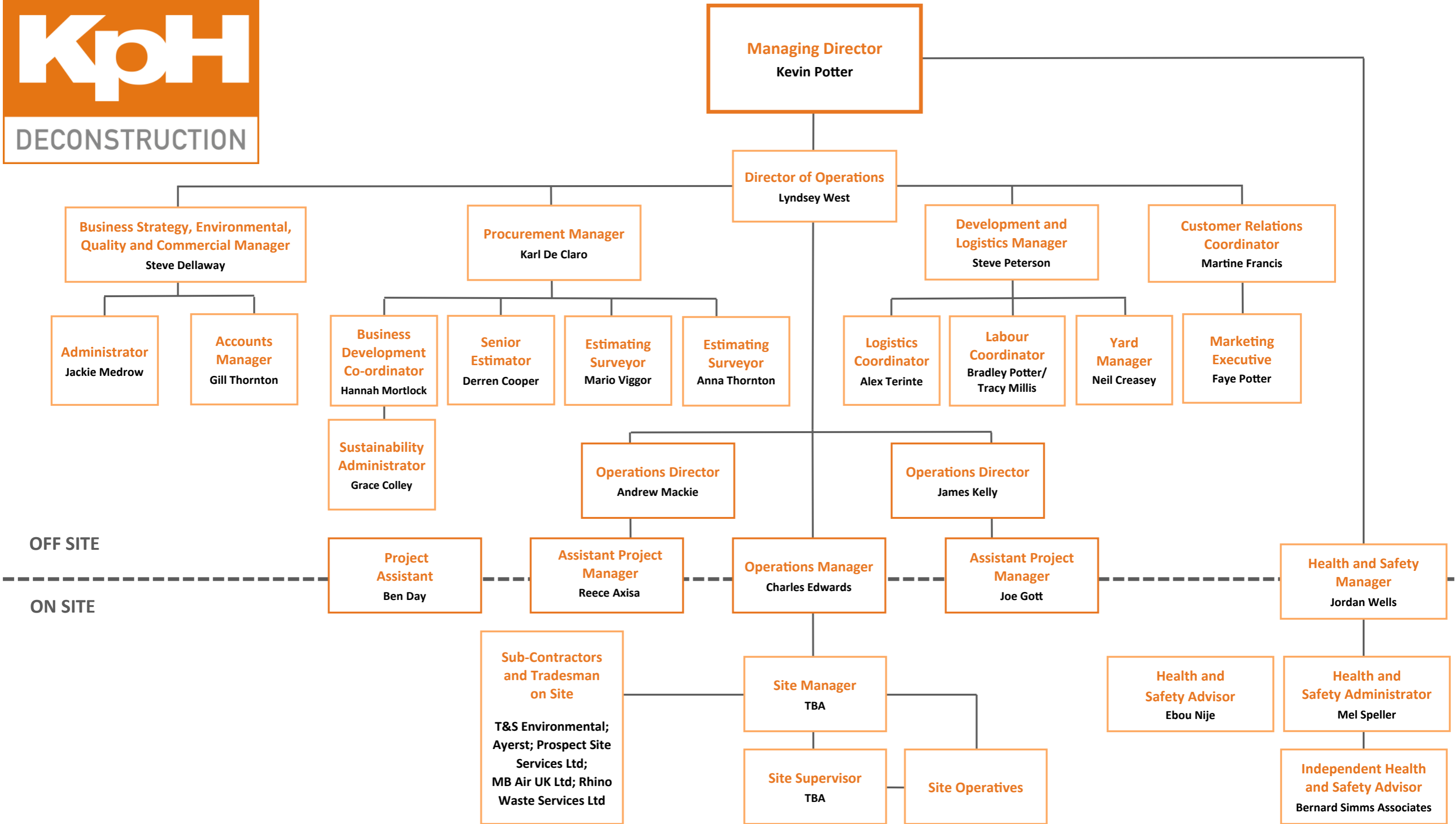
Facial hair fashion or cultural non-religious practice in this respect will not be accepted as a reason for non-compliance.

Please remember this is to protect you from acute or chronic health effects of exposure to airborne hazards. For which we have a legal and moral duty to control.

Signed for KpH Group Limited:

Jordan Wells Health and Safety Manager	<i>Jordan Wells</i>
Date:	01/04/2022

ORGANISATION CHART - KPH DECONSTRUCTION SERVICES LTD



"Working safely for our future"

KpH Organisation Chart Deconstruction / October 2021

