HOPE CEMENT LIMITED

DATA PROTECTION COMPLIANCE POLICY

About this policy

Any organisation which processes any personal data (whether that personal data is held in a paper or electronic format e.g. on computers, laptops, ipads, smartphones, electronic networks, CDs, USBs etc.) must comply with the European Data Protection Directive (95/46/EC) (the "**Directive**"), which is implemented in the UK by the Data Protection Act 1998 (the "**Data Protection Laws**"). Accordingly Hope Cement Limited and its group companies (referred to in this policy as "**Hope**") and each staff member must comply with the Data Protection Laws.

To help achieve compliance with the Data Protection Laws, this policy sets out what Hope and each staff member needs to do when processing personal data. The types of personal data that we may typically handle include details of current, past and prospective staff members as well as personal data about other individuals with whom we deal, such as, for example, customers, suppliers, contracted hauliers and their employees.

This policy covers:

Topic	Page number
Who does this policy apply to?	3
Consequences of breaching the Data Protection Laws and this policy	3
Terms used in the Data Protection Laws and this policy	3
The Data Protection principles	6
How do I process personal data fairly and lawfully (Principles 1 and 2)?	7
How do I ensure processing is adequate, relevant and not excessive (Principle 3)?	10

How do I keep personal data accurate and up to date (Principle 4)?	10
How do I ensure that personal data is not kept longer than necessary (Principle 5)?	10
How do I process data in accordance with data subjects' rights (Principle 6)?	11
What security measures must I comply with (Principle 7)?	12
When can I transfer personal data outside of the EEA (Principle 8)?	13

Who does this policy apply to?

This policy applies to all staff members. For the purposes of this policy, "staff member" means all of Hope's permanent and temporary employees, and any other individuals who are working for the company but are not directly employed, including company officers, consultants, contractors, contracted hauliers and their employees, work experience candidates and agency workers. Use of the term "staff member" is not to be taken to imply that any particular individual has employment status with the company. When we refer to “you” in this policy, we mean each individual staff member.

Compliance Team

If there is anything in this policy which you do not understand or you have questions about, or if you are in any way uncertain as to what you must do in order to ensure compliance with the Data Protection Laws, then contact the Compliance Team for assistance. Contact details for the Compliance Team are given at the end of this policy document.

Consequences of breaching the Data Protection Laws and this policy

Breaches of the Data Protection Laws can result in enforcement action by the Information Commissioner against Hope, and in serious cases the Information Commissioner has power to impose fines of up to £500,000. Data protection laws in the EEA will change in the near future, when the new EEA Data Protection Regulation replaces the existing Directive. The Regulation will mean even more stringent compliance obligations and even bigger fines for data protection breaches: up to 4% of annual global turnover. Further, some breaches of the Data Protection Laws are a criminal offence. Consequently any breach of this policy may result in disciplinary action by the company.

Terms used in the Data Protection Laws and in this policy

This section gives definitions of the terms used in the Data Protection Laws and which are used in this policy.

Term	Definition
Personal Data	Means information from which a living individual can be identified. This includes factual information such as telephone numbers, bank account details, credit card numbers, names, addresses, e-mail addresses, photographs, CCTV footage, voice recordings and vehicle tracking data. It also includes expressions of opinion and indications of intentions about individuals (and their own expressions of opinion/intentions), such as performance appraisals. Information which does not on its own identify an individual is still 'personal data' for the purposes of the Data Protection Laws if it can be combined with other information that Hope holds or that Hope could obtain fairly easily. For example, if personal data has been anonymised by Hope but the company also holds the key to 'de-anonymise' the information, or could fairly easily obtain that key, then the anonymised information will still be personal data for the purposes of the Data Protection Laws.
Sensitive Personal Data	Information relating to: • Racial or ethnic origin; • Political opinions;

	• Religious beliefs or beliefs of a similar nature; • Trade union membership; • Physical or mental health or condition; • Sexual life; or • Offences or alleged offences or information relating to any proceedings for offences committed or allegedly committed.
Processing	The term 'processing' covers virtually anything you can do with personal data (whether processed in an electronic format or in a structured paper-based format), including: • Obtaining, recording, retrieving, consulting or holding it; • Organising, adapting or altering it; • Disclosing, disseminating or otherwise making it available; and • Aligning, blocking, erasing or destroying it.
Data Subject	This is the individual to whom the personal data relates.
Data Controller	A party who (either alone or jointly) determines the purposes for which and the manner in which any personal data is, or will be, processed. Hope is a data controller.
Data Processor	A party who processes personal data on behalf of a data controller (other than an employee of the data

	controller). For example, some of our suppliers (such as our payroll providers, expenses system providers, healthcare providers, pension providers, IT helpdesk and our telephony providers) are data processors for Hope.
European Economic Area or "EEA"	Means European Union member states plus Norway, Liechtenstein and Iceland.

The Data Protection principles

The Data Protection Laws contain eight principles that all data controllers must comply with when processing personal data. The table below gives a high level summary of the principles. The sections that follow describe how you apply those principles in practice.

EIGHT DATA PROTECTION PRINCIPLES	
1	Personal data must be processed fairly and lawfully;
2	Personal data must be obtained for one or more specified and lawful purposes and must not be processed incompatibly with those purposes;
3	Personal data must be adequate, relevant and not excessive in relation to the purposes for which the data are processed;
4	Personal data must be accurate and kept up to date;
5	Personal data must not be kept for longer than is necessary;
6	Personal data must be processed in accordance with the rights of the data subject under the Data Protection Laws;
7	Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data as well as against

	accidental loss, destruction of or damage to that data; and
8	Personal data must not be transferred outside of the EEA unless the recipient provides an adequate level of protection in line with the Data Protection Laws.

How do I process personal data fairly and lawfully (Principles 1 and 2)?

To process personal data **fairly**, you need to make sure that you only process personal data if the data subject has been told:

- who the data controller is (in this case Hope);
- the purpose for which the data is to be processed by Hope; and
- the identities of anyone to whom the data may be disclosed or transferred.

This information is contained in so-called "privacy notices" which we give to staff members, applicants and any other individuals about whom we process personal data. You must ensure that you are familiar with our privacy notices and do not process personal data for any purpose other than those contained in the privacy notices. Our general privacy notice can be found on our website at www.breedongroup.com and is set out in the Appendix to this Policy.

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Data Protection Laws. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before carrying out any new processing, except in certain circumstances where a legal exemption from this obligation applies.

You should only collect the minimum amount of personal data necessary for your purpose. In particular, please be cautious when inputting information about individuals into Customer Relationship Managememt ("CRM") systems/contacts databases. Do not include information that is not required, e.g. notes/observations about an individual, because this could go beyond the purpose for which the data was originally collected and may result in a claim against Hope for unlawful processing of personal data.

To process personal data lawfully, Hope must meet certain conditions that are set out in the Data Protection Laws. Those conditions which are most relevant to us as an organisation are summarised in Tables A and B below. Please consult the Compliance Team about any other conditions that may apply when processing personal data.

One of the conditions for processing personal data is that the data subject has given their consent to such processing. Relying on consent to process personal data may be appropriate in some circumstances, but keep in mind that if other conditions are relevant they should be relied on instead – in other words, consent is a condition of 'last resort'. Also note that the consent must be fully informed, i.e. the data subject must know what they are consenting to, and the data subject must have a genuine choice as to whether to give consent or not.

IMPORTANT

When processing **non-sensitive personal data**, you must make sure that **at least one of the conditions in Table A** applies.

When processing **sensitive personal data**, **you must make sure that one of the conditions in Table A applies and at least one of the conditions in Table B also applies**. The conditions in Table B are fairly limited, so when processing sensitive personal data it is likely that we will need to get written consent from the data subject to enable their sensitive personal data to be processed.

TABLE A – Key conditions for processing <u>any</u> personal data (one or more must apply)

Business Interests	Processing is carried out in order to pursue Hope's legitimate business interests: e.g. collecting personal data from our customers/clients so that Hope can provide its products/services. Much of the processing of personal data that Hope does as an organisation falls under this condition. This condition only applies if the processing does not adversely affect the individual concerned. If there is a serious mismatch of competing interests between the business and the individual, the individual's interests will have priority over business interests. If you are unsure whether there are competing interests, please contact the Compliance Team.
Contracts	Processing is carried out in order to enter into a contract between Hope and the data subject or to perform such a contract.
Legal Obligations	Processing is carried out in order to comply with legal obligations placed on Hope. This does not apply to contractual obligations.
Vital Interests of Data Subject	Processing is carried out in order to protect the data subject's vital interests: e.g. where an individual's personal data needs to be disclosed in a medical emergency.

TABLE B – Key conditions for processing <u>sensitive</u> personal data (one or more must apply)

Employment Obligations	Processing is carried out by Hope in the exercise of its legal obligations or rights in connection with employment such as sick pay administration, or checking that an individual is eligible to work in the UK.
Equal Opportunities	Processing is carried out in order to monitor equal opportunities within Hope in respect of race or ethnic origin.
Legal Rights	Processing is carried out in order to establish, exercise or defend the legal rights of Hope.
Publicly Available Information	The personal data has been made public as a result of steps deliberately taken by the data subject. Be cautious where relying on this condition – information available publicly such as on the internet, may not have been made public by the data subject themselves, in which case this condition would not apply.

Vital Interests of Data Subject	Processing is carried out in order to protect the data subject's vital interests: e.g. where an individual's sensitive personal data needs to be disclosed in a medical emergency.

How do I ensure processing is adequate, relevant and not excessive (Principle 3)?

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any personal data which is not necessary for that purpose should not be collected in the first place.

As well as ensuring that any personal data which you process is necessary and relevant for the purpose for which you are processing it, you must at the same time ensure that you have adequate personal data for your purpose. In other words, you should obtain enough information about an individual to enable you to perform your purpose(s) but no more.

How do I keep personal data accurate and up to date (Principle 4)?

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out of date personal data should be destroyed or erased from Hope's systems.

Although ultimately it is Hope's responsibility to make sure personal data is up to date and accurate, Hope will often be reliant on data subjects themselves to tell us of changes to their personal data. From a practical perspective it is often useful to encourage data subjects to contact us if personal data we hold about them becomes out of date or if they are aware of any inaccurate data we hold about them.

If you are involved in planning an activity or project that includes processing of personal data, think about appropriate methods that can be implemented easily to encourage data subjects to notify us about changes to their personal data.

How do I ensure personal data is not kept for longer than necessary (Principle 5)?

Personal data should not be kept longer than is necessary for the purpose for which it was obtained. This means that personal data should be destroyed or erased from our systems when it is no longer required.

You must consider whether there are any data retention practices and procedures that are specific to your department, and with which you will need to comply. It may also be the case that you will need to make decisions about how long to keep certain personal data on a case by case basis. If you are unsure about whether certain personal data should be retained, you should contact the Compliance Team.

How do I process data in accordance with data subjects' rights (Principle 6)?

Data Subjects are granted various rights by the Data Protection Laws. The key rights, and the actions you need to take when they are exercised, are as follows:

(a) The right to ask to see what personal data Hope holds about them. Please refer any written requests to the Compliance Team immediately as Hope has only up to 40 days in which to respond to such requests.

Sometimes requests for personal data may be made over the telephone – in which case you should:

(i) Check the caller's identity to make sure that information is only given to a person who is entitled to it.

(ii) Ask the caller to put their request in writing if you are not sure about the caller's identity and where their identity cannot be checked.

(iii) Refer to the Compliance Team for assistance in difficult situations. No-one should be bullied into disclosing personal data.

(b) The right to require Hope to rectify any personal data which is inaccurate. For example, if you are requested to change an address of a customer/client or supplier etc, you should make those changes immediately. If inaccurate personal data about a data subject has been passed on to a third party, it may also be necessary to take steps to correct the third party's data, depending on the nature of the data and whether the third party is still likely to be using it.

(c) The right to prevent processing of their personal data if this has caused or is likely to cause damage or distress. Please contact the Compliance Team if you receive a request to prevent processing.

(d) The right to ask for the logic involved in any automated decision taken without human input, i.e. by a computer. Again, please contact the Compliance Team if you receive such a request.

(e) The right to prevent Hope sending unsolicited marketing materials to them. Depending on the type of unsolicited marketing, intended recipients may have a right to either opt-in or opt-out. Please contact the Compliance Team if you intend to send any unsolicited marketing to named individuals.

What security measures must I comply with (Principle 7)?

Personal data must be kept secure from unauthorised access and from being accidentally lost, destroyed or damaged. To do this, you should follow all applicable company security guidelines and procedures and all company policies that have a bearing on data security.

Do not disclose any personal data internally or externally to a third party (i.e. a person or organisation) unless one or more of the following apply:

(a) Either the data subject has been informed in a privacy notice that his or her personal data may be disclosed to such parties and the purpose for which it is being disclosed, or the disclosure takes place in the course of conducting Hope's legitimate business activities and the data subject would expect their personal data to be used for this purpose;

(b) The disclosure is made with the consent of the data subject to whom the personal data relates. If you are disclosing sensitive personal data, you must obtain written consent to disclosure;

(c) The disclosure will be to an organisation and/or individual entitled to receive the personal data, for example, to the Police where the information is necessary to prevent or detect crime, or to the tax authorities;

(d) The disclosure is made in order to comply with legal obligations placed on Hope or to comply with a court order;

(e) The disclosure is made in the course of proceedings in court; or

(f) The Compliance Team has authorised the disclosure.

Any disclosure of personal data must be subject to appropriate security safeguards and, depending on the nature of the personal data, confidentiality obligations. In particular, any internal communications about a staff member's salary, benefits or any other information about Hope's staff members should be communicated securely and in confidence.

If the disclosure is to a third party that provides services to Hope which include the processing of personal data in respect of which Hope is the data controller, only such personal data as is necessary should be disclosed to the relevant third party, and a 'Data Processor Agreement' must be put in place between Hope and that third party. A Data Processor Agreement ensures that the third party is contractually obliged to comply with legally-specified minimum data protection requirements and to put appropriate security measures in place. You must contact the Compliance Team in all cases where a Data Processor Agreement is required, and the Compliance Team will provide the necessary contract terms.

If you are uncertain about disclosing any personal data to third parties you should contact the Compliance Team for guidance.

When can I transfer personal data outside the EEA (Principle 8)?

Do not transfer personal data to a country outside of the EEA (European Economic Area) unless:

(a) it is to perform a contract with the data subject; or

(b) the data subject has consented; or

(c) the country is on the Information Commissioner's approved countries list (please contact the Compliance Team for details of approved countries); or

(d) a contract has been put in place with the third party/third parties to which the personal data will be transferred, in the form of the European Commission's relevant approved standard contract for transfers of personal data outside of the EEA (known as "**Model Contracts**").

Note that a transfer of personal data outside of the EEA not only includes sending relevant data to an entity in a non-EEA country (e.g. by email) but also includes allowing access to that data from outside the EEA. For example, where a Hope group company holds or transfers personal data on or to servers in the EEA, and the data is then accessible by individuals in a non-EEA country, this is considered to be a transfer of data to that non-EEA country.

If you are considering a transfer of personal data outside the EEA, or are unsure about whether such a 'transfer' of personal data will take place, contact the Compliance Team for advice.

COMPLIANCE TEAM

CONTACT DETAILS

Name	Office	Telephone and e-mail
Ross McDonald Chief Compliance Officer and Company Secretary	Breedon on the Hill, Derby, DE73 8AP	D: 01332 694404 ross.mcdonald@breedongroup.com
Steve Tagg Human Resources Director	Breedon on the Hill, Derby, DE73 8AP	T: 01332 694000 steve.tagg@breedongroup.com
Lorna Bennett Commercial Solicitor	Hope Works, Hope Valley, Derbyshire, S33 6RP	D: 01433 622323 M: 07802 873723 lorna.bennett@breedongroup.com
Melanie Haycox Company Registrar	Home Based	M: 07545 920933 melanie.haycox@breedongroup.com

APPENDIX

(Privacy Notice)

Purpose of this privacy notice

The Data Protection Act 1998 (the "**DPA**") imposes legal obligations on the way in which Hope Cement Limited ("Hope") obtains, records and processes personal information about staff members. This notice explains:

- what personal information Hope collects and for what purposes; and
- your rights in respect of our use of your personal data.

For the purposes of this policy, "staff member" means all of Hope's permanent and temporary employees, and any other individuals who are working for the company but are not directly employed, including company officers, consultants, contractors, contracted hauliers and their employees, work experience candidates and agency workers.

When we refer to “you” in this policy, we mean each individual staff member. Use of the term 'staff member' is not to be taken to imply that any particular individual has employment status with the company.

This policy covers:

Topic
Terminology
What do we use your personal data for?
Who may have access to your personal data?
Monitoring
Your rights

Terminology

Please familiarise yourself with the following words and phrases as they have particular meanings in the DPA and are used throughout this privacy notice:

Personal Data	Means any information from which a living individual can be identified. This includes factual information such as telephone numbers, bank account details, credit card numbers, names, addresses, e-mail addresses, photographs, video monitoring equipment ("CCTV") footage, voice recordings and vehicle tracking data. It also includes expressions of opinion and indications of intentions about individuals (and their own expressions of opinion/intentions), such as performance appraisals. Information which does not on its own identify an individual is still "personal data" for the purposes of the DPA if it can be combined with other information that Hope holds or that Hope could obtain fairly easily. For example; if personal data has been anonymised by Hope but the company also holds the key to "de-anonymise" the information, or could fairly easily obtain that key, then the anonymised information will still be personal data for the purposes of the DPA.
Sensitive Personal Data	Information relating to: • Racial or ethnic origin; • Political opinions; • Religious beliefs or beliefs of a similar nature; • Trade union membership; • Physical or mental health or condition; • Sexual life; or • Offences or alleged offences or information relating to any proceedings for offences committed or allegedly committed.
Processing	The term "processing" covers virtually anything you can do with personal data (whether processed in an electronic format or in a structured paper-based format) including: • Obtaining, recording, retrieving, consulting or holding it;

	• Organising, adapting or altering it; • Disclosing, disseminating or otherwise making it available; and • Aligning, blocking, erasing or destroying it.
Data Subject	This is the individual to whom the personal data relates.
Information Commissioner	The UK Information Commissioner, who is responsible for implementing, overseeing and enforcing the DPA.

What do we use your personal data for?

We may process personal data about you for the following purposes:

EMPLOYEES	
Payroll, Pension, Tax and Accounts	To calculate and pay your salary, PAYE, NI, and pension contributions, and to keep business accounts.
Benefits	To calculate, pay and provide benefits such as life assurance, private medical cover, bonuses and other benefits that Hope may offer from time to time, such as cycle to work scheme and childcare voucher scheme.
Employee Administration	To administer your employment with us. For example, this will include, complying with employment contracts, legal obligations, our policies and to administer medical and sickness records, sick pay/leave information, holiday/absence, appraisals, promotions, disciplinary and grievance matters, family leave, applications/interview records, working time records and immigration checks.
Administration of Membership Records	To administer your membership with clubs, associations and other organisations for business and/or professional purposes.
Training and Career Development	To administer and supervise your training and career development.
Trade Unions	To facilitate trade union memberships and relationships. This might include the processing of sensitive personal data.
Medicals	To carry out medical examinations to ensure that you are able to carry out the duties which form part of your duties at work, obtaining medical reports if you are on long term sick and drug and alcohol testing**.**

INDIVIDUALS WHO ARE NOT EMPLOYED BY THE COMPANY	
Remuneration and Accounts	To calculate and/or pay your charges/fees/expenses/allowances and to keep business accounts.
Personnel Administration	To administer your work with us. For example, this will include, monitoring compliance with contracts for services, legal obligations and, where relevant, our policies.
Training	To provide you with our company training relevant to the services which you provide.
ABOUT ALL STAFF MEMBERS	
Security	To keep your personal data and that of others secure and prevent unauthorised access, loss, damage, destruction or corruption.
Business Development	To develop our business generally including through marketing (i.e. we may provide your name, work contact details and/or experience to existing and potential customers/clients/suppliers).
Business Travel	To administer any travel and/or accommodation arrangements where you are required to travel within or outside the UK.
Company and Group Company Administration	To carry out administration tasks within Hope and its group companies.
Prevention and Detection of Crime	To prevent and detect crime. This might include processing sensitive personal data including information about offences or alleged offences and information relating to any proceedings for offences committed or allegedly committed.
Equal Opportunities	To promote and monitor equal opportunities within Hope. This might include the processing of sensitive personal data including, religious or similar beliefs, and

	ethnic origin.
Corporate finance, Mergers and Acquisitions	To carry out group company or business restructuring, to sell or otherwise dispose of any of the Hope companies or businesses, or acquire or merge with other companies or businesses. We may disclose your personal data, including sensitive personal data, for any of the above purposes, including at negotiation stage.
Regulatory and Professional Requirements	To comply with regulations and professional requirements to which Hope is subject.
Tax	To administer revenue and tax obligations.
Vetting	To carry out vetting of staff members to comply with relevant legal requirements. This might include processing sensitive personal data including information obtained from CRB or other official checks about offences or alleged offences and information relating to any proceedings for offences committed or allegedly committed.
Health and Safety	To comply with health and safety laws and Hope's SHE policies. This may include Hope processing your sensitive personal data, such as details of your mental and physical health.
Monitoring	To monitor your use of Hope's IT resources. More information has been provided about this in the section headed 'Monitoring' below.

Who may have access to your personal data?

Sometimes we may need to disclose some of your personal data to other third party organisations. Depending on your status or role with the company, this may happen where we use another organisation to provide services, such as payroll administrators, pension administrators, life assurance providers, expenses administrators, IT service providers, training providers, recruitment agencies, professional advisers (including lawyers and accountants), occupational health professionals, banks, vehicle providers, auditors, or other contractors.

We may also have to disclose some personal data to professional bodies, HM Revenue & Customs, Courts, the Police and other UK governmental or regulatory authorities.

From time to time, we may need to transfer your personal data outside the EEA, for example, where we need to share the information about our staff members with Hope's shareholders or directors outside the EEA.

Additionally, we may use service providers that are based outside of the EEA, or which are part of global groups of companies, but we will ensure that any such service provider complies with strict obligations of confidentiality and security, and that any transfers of personal data outside the EEA comply with the law.

Please be aware that your name and work contact details and other information about your work life (for example experience) may be made available to customers/clients, potential customers/clients, suppliers and potential suppliers, as well as being available to other staff members within Hope, e.g. via our company directory.

If you have any objections to any disclosures of your personal data, including on our intranet or website, please contact the Compliance Team. Contact details for the Compliance Team are given at the end of this policy document.

Monitoring

Where relevant, we may monitor your use of our IT resources and communications, including computers, internet and intranet access, e-mail, voicemail, faxes, telephones (including company mobile phones), and data collected by CCTV systems, access card systems, and vehicle mounted tracking and camera systems for the following reasons**:**

IT Maintenance	To maintain and update IT resources and to monitor for viruses and other disruptive programmes.
Crime	To investigate, detect and prevent crime and to identify, find and prosecute offenders. This might include the use of CCTV (see below for more detail), for example, to protect staff members' and other individuals' safety.
Unauthorised use of IT resources	To determine whether any IT resources are being used without authorisation either by staff members or external hackers.
Information Gathering	To establish the existence of business related facts and/or to determine whether communications are relevant to our business. For example, depending on your status or role with the company, if you are away from work, to establish whether incoming e-mails are from customers/clients and to ensure that they are properly dealt with during your absence.
Legal and Policy Compliance	To determine whether Hope and/or its staff members are complying with legal requirements, contracts, our relevant policies and rules and any other requirements with which Hope and/or its staff members should comply.
Material Quality and Service Standards	To determine whether you are attaining the targets/standards which you ought to be achieving, such as customer/client material quality and service standards.

We may also use CCTV to monitor staff members and others on our premises and may disclose footage to third parties such as the Police, solicitors and the Courts. We may also disclose CCTV footage to the media if we believe that this will assist in finding or identifying criminals. Any third parties operating our CCTV system or editing footage for us may also have access to footage on which you appear.

Any CCTV monitoring carried out by Hope will be subject to the CCTV Code of Practice which has been issued by the Information Commissioner. If you would like to see a copy of the CCTV Code of Practice, please contact the Compliance Team.

Please see our CCTV/Access Card/Vehicle Mounted Tracking and Camera Monitoring Policy for guidance on compliance with data protection obligations when CCTV is used by Hope. This policy is available from the Compliance Team, and posted on the Hope website.

Hope operates a telephony system on which calls are recorded for purposes including the verifying of service and delivery instructions, and monitoring compliance with contracts and customer and client service and quality standards by Hope employees, contracted hauliers and drivers. Telephone recordings may be disclosed to operations, legal, sales, logistics, and health and safety staff, as well as to Hope's customers, and also to the same categories of third parties and for the same purposes as CCTV footage. Hope's telephony provider may also have access to telephone recordings.

Hope also operates vehicle mounted tracking and camera systems. Data gathered by such systems may be used for monitoring compliance with: contracts, service and delivery standards, materials quality standards and safety standards (for example, safe driving standards) by Hope employees, contracted hauliers and drivers; and for monitoring the deployment of transport resources available to the Company for the purposes of its business. Such data may be disclosed to operations, legal, sales, logistics and health and safety staff, as well as to Hope's customers and also to the same categories of third parties and for the same purposes as CCTV footage. Hope's vehicle tracking and camera system provider may also have access to this data.

Your rights

As a data subject, you have the following rights under this policy, which are granted by the DPA:

- the right of access to personal data relating to you (see below);
- the right to prevent your personal data being processed (see below);
- rights in relation to automated decision taking (see below);
- the right to have inaccurate personal data corrected or erased (see below); and
- compensation for damage caused by contravention of the DPA.

These rights are explained in more detail below, but if you have any comments, concerns or complaints about Hope's use of your personal data, please contact the Compliance Team.

Requests for access to your personal data

You may ask to see what personal data we hold about you and be provided with:

- a copy;
- details of the purpose for which it is being or is to be processed;
- details of the recipients or classes of recipients to whom it is or may be disclosed; and
- any information available about the source of that data.

Requests for your personal data must be made to the Compliance Team in writing and a copy may be retained on your personnel file.

To help us find the information easily, please give us as much information as possible about the type of information you would like to see.

If, to comply with your request, we would have to disclose information relating to or identifying another person, we may need to obtain the consent of that person if possible. If we cannot obtain consent, we may need to withhold that information or edit the data to remove the identity of that person if possible.

There are certain types of data which we are not obliged to disclose to you, which include:

- confidential references we give;
- personal data processed for the purposes of management forecasting or management/succession planning where disclosure would cause harm; and
- personal data which records our intentions in relation to any negotiations with you where disclosure would be likely to prejudice those negotiations.

Right to prevent processing of personal data

You may request that we stop processing your personal data or require that processing is stopped if that processing is causing or is likely to cause you or someone else substantial damage or distress, and that damage or distress is or would be unwarranted.

If you think that any of our processing may cause such damage or distress, you should notify the Compliance Team in writing.

Rights in relation to automated decision taking

You may ask us to ensure that, when we are evaluating you (for example evaluating your conduct or your performance), we don't base any decisions solely on an automated process. You must notify us of this request in writing to the Compliance Team.

If you make such a request, you will then have the right to be notified where such a decision is or will be based on an automated process. If we notify you that we have taken such a decision, you may request us to review that decision other than by automatic means by writing to the Compliance Team within 21 days of receiving the notification.

These rights will not apply in all circumstances, for example where the decision is authorised or required by law and steps have been taken to safeguard your interests.

Inaccurate data

You may challenge the accuracy of personal data which we process about you. If, on investigation, it is found that personal data is inaccurate, you are entitled to have the inaccurate data removed or corrected, as appropriate, and to receive written confirmation that this has been done.

Your responsibilities

You must carry out your duties in such a way to ensure that Hope complies with its obligations under the DPA. Where you are processing personal data about another person, it is your responsibility to ensure that the personal data is:

- processed fairly;
- processed for the limited purposes which Hope has registered with the Information Commissioner;
- adequate, relevant and not excessive for those purposes;
- accurate;
- not kept longer than is necessary;
- processed in accordance with the DPA;
- kept secure; and
- not transferred outside the European Economic Area (EEA) without the required safeguards.

These responsibilities are explained in detail in our **"Data Protection Policy"**, a copy of which is available from the Compliance Team, and posted on the Hope website.

COMPLIANCE TEAM

CONTACT DETAILS

Name	Office	Telephone and e-mail
Ross McDonald Chief Compliance Officer and Company Secretary	Breedon on the Hill, Derby, DE73 8AP	D: 01332 694404 ross.mcdonald@breedongroup.com
Steve Tagg Human Resources Director	Breedon on the Hill, Derby, DE73 8AP	T: 01332 694000 steve.tagg@breedongroup.com
Lorna Bennett Commercial Solicitor	Hope Works, Hope Valley, Derbyshire, S33 6RP	D: 01433 622323 M: 07802 873723 lorna.bennett@breedongroup.com
Melanie Haycox Company Registrar	Home Based	M: 07545 920933 melanie.haycox@breedongroup.com