

COLLEAGUE DATA PRIVACY NOTICE (UK Based Colleagues)

1. INTRODUCTION

- 1.1 CPPGroup Limited and our associated companies (including Card Protection Plan Limited, Homecare Insurance Limited, CPP Assistance Services Limited, Blink Innovation (UK) Limited and CPPGroup Services Limited ("**Company**", "**we**", "**us**" and "**our**") hold and process data on all current/former colleagues, individual contractors, applicants, interns, consultants and directors, and third parties whose information you provide to us in connection with the employment or other work relationship (e.g. next-of-kin, emergency contact information and/or dependents) ("**staff**" or "**you**" or "**your**").
- 1.2 We take your data protection rights and our legal obligations seriously. Your personal data will be treated in a secure and confidential manner and only as set out below or otherwise notified to you in writing.
- 1.3 The following Data Privacy Notice describes the categories of personal data we may process within all Group companies. It also describes how your personal data may be processed, for what purposes we process your data and how your privacy is safeguarded during our relationship with you. It is intended to fulfil our obligations to provide you with information about the Company's processing of your personal data under privacy laws. Please note that it does not form part of your contract of employment or engagement. Where we use the term employment in this Data Privacy Notice this also includes other engagements (such as contractors) or work relationships.
- 1.4 If you have any questions regarding the processing of your personal data or if you believe your privacy rights have been violated, please contact dataprivacy@cpp.co.uk. If you are aware of an unauthorised use or disclosure of data, please contact dataprivacy@cpp.co.uk.

2. PROCESSING OF PERSONAL DATA

- 2.1 The Company collects and processes your personal data for the purposes described in this Data Privacy Notice.
- 2.2 The Company or relevant associated company of the Company identified in your employment contract or contract for services will be the data controller of your personal data. In addition, where processing of personal data is undertaken by other associated companies of the Company for their own independent purposes, these associated companies may be controllers of your personal data. These companies include CPPGroup Limited, CPPGroup Services Limited, Card Protection Plan Limited, CPP Assistance Services Limited, CPP Secure Limited and Homecare Insurance Limited.

3. WHAT DATA DO WE PROCESS?

- 3.1 We may collect various types of personal data about you for the purposes described in this Data Privacy Notice including:
 - 3.1.1 **Personal details:** including your name (previous and current), gender, nationality, date of birth, age, personal contact details (e.g. address, phone number), National Insurance number, immigration and eligibility to work information, driving licence, emergency contact information, details of any disability and any subsequent reasonable adjustments required;
 - 3.1.2 **Recruitment and selection data:** skills/experience, qualifications, references, CV, application, interview and assessment data, vetting and verification information (e.g. results of credit reference check), right to work verification, information related to the outcome of your application, details of any offer made to you;

- 3.1.3 **Data related to your engagement:** contract of employment or engagement, work contact details, colleague number, photograph, various system IDs, your contracted business entity, your reporting line, your colleague/contingent worker type, your start date and end dates, the reason for termination, your terms and conditions of employment/engagement, your cost centre, your job title and job description, exit interviews, references to be provided to prospective employers, the reason for any change in job and date of change;
- 3.1.4 **Regulatory data:** records of your registration with any applicable regulatory authority, your regulated status and any regulatory certificates and references;
- 3.1.5 **Remuneration and benefits data:** your remuneration information (including salary information as applicable, allowances, overtime, bonus and commission plans), payments for leave/absence (e.g. holiday pay, sick pay, family leave pay), bank account details, grade, National Insurance number, tax information, third party benefit recipient information (e.g. expression of wish and dependents information), details of any benefits you receive or are eligible for, benefit coverage start date, expense claims and payments, loans, deductions, salary sacrifice arrangements, childcare vouchers, share scheme participation, information and agreements;
- 3.1.6 **Long-Term Incentive Plans** (where applicable): name, address, date of birth, National Insurance Number, leave date (where relevant), payroll number, personal share reference number, date options granted and number of shares granted.
- 3.1.7 **Leave data:** attendance records, absence records (including dates and categories of leave/time-off requests and approvals), holiday dates, requests and approvals and information related to family leave or other special or statutory leave;
- 3.1.8 **Absence management data:** absence history, fit notes, details of absence reasons, details of reasonable adjustments, details of treatment and prognosis, manager and People communications, return to work interviews, meeting records, medical reports, occupational health reports (where relevant);
- 3.1.9 **Flexible working procedure data:** requests, consideration, correspondence, meeting notes and outcome records;
- 3.1.10 **Restructure and redundancy records:** change plans, organisation charts, consultation records, selection and redeployment data;
- 3.1.11 **Performance management data:** colleague and manager feedback (where relevant); your performance review information, outcomes and objectives; talent programme assessments and records; succession plans; formal and informal performance management process records;
- 3.1.12 **Training and development data:** data relating to training and development needs or training received or assessments completed;
- 3.1.13 **Disciplinary and grievance data:** allegations, complaints, investigation and proceeding records and outcomes;
- 3.1.14 **Health and safety data:** health and safety audits, health and safety screening requests and results, DSE/risk assessments, incident reports;
- 3.1.15 **Monitoring data (to the extent permitted by applicable laws):** closed circuit television footage, system and building login and access records (York only), download and print records, call (York only) or data caught by IT security programmes and filters,
- 3.1.16 **Colleague claims, complaints and disclosures information:** subject matter of employment or contract based legal action and complaints, pre-claim conciliation, communications, settlement discussions, claim proceeding records, colleague involvement in incident reporting and disclosures;

- 3.1.17 **Equality and diversity data:** where permitted by law and provided voluntarily, data regarding gender (stored for Gender Pay Reporting purposes);
- 3.1.18 Any other personal data which you choose to disclose to us during the course of your engagement whether verbally or in written form (e.g. by email);
- 3.2 Certain additional information may be collected where this is necessary and permitted by local applicable laws.

4. SPECIAL CATEGORIES OF DATA

- 4.1 To the extent permitted by applicable laws the Company may collect and process a limited amount of personal data within the above data listed at 3.1 falling into special categories, sometimes called "sensitive personal data". This term means information relating to:
 - 4.1.1 racial or ethnic origin;
 - 4.1.2 political opinions;
 - 4.1.3 religious or philosophical beliefs;
 - 4.1.4 physical or mental health (including details of accommodations or adjustments);
 - 4.1.5 trade union membership;
 - 4.1.6 sexual orientation; and
 - 4.1.7 criminal records and information regarding criminal offences or proceedings.

5. HOW DOES THE COMPANY COLLECT DATA?

- 5.1 The Company collects and records your personal data from a variety of sources, but mainly directly from you. You will usually provide this information directly to your managers or local People contact or enter it directly into our systems (e.g. through your self-service access to Cascade) your participation in People processes, emails and instant messages you send or through verbal information which may be recorded electronically or manually. In addition, further information about you will come from your managers, the People Team or occasionally your colleagues.
- 5.2 We may also obtain some information from third parties: e.g. references from a previous employer, medical reports from external professionals, information from HMRC, benefit providers or where we employ a third party to carry out a background check (where permitted by applicable law) or occasionally from clients.
- 5.3 In some circumstances, data may be collected indirectly from monitoring devices or by other means (e.g. building and location access control and monitoring systems, CCTV, telephone recordings, instant message logs and email and Internet access logs), if and to the extent permitted by applicable laws. In these circumstances, the data may be collected by the Company or a third party provider of the relevant service. This type of data is generally not accessed on a routine basis but access is possible. Access may occur, for instance, in situations where the Company is investigating possible violations of Company policies such as those relating to the use of the telephone system and the Internet, or colleague conduct generally, or where the data are needed for compliance or billing purposes. More frequent access to such data may occur incidental to an email surveillance program, if and to the extent permitted by applicable laws. Please refer to the Group Acceptable Use Policy.
- 5.4 Where we ask you to provide personal data to us on a mandatory basis, we will inform you of this at the time of collection and in the event that particular information is required by the contract or legislation this will be confirmed. Failure to provide any mandatory information will mean that we cannot carry out certain People processes (e.g. if you do not provide us with your bank details, we will not be able to pay you). In some cases it may mean that we are unable to continue with your employment or engagement as the Company will not have the personal data we believe to be necessary for the effective administration and management of our relationship with you.

- 5.5 Apart from personal data relating to you, you may also provide the Company with personal data of third parties, notably your dependents and other family members, for purposes of People administration and management, including the administration of benefits and someone to contact in an emergency. Before you provide such third party personal data to the Company you must first inform these third parties of any such data which you intend to provide to the Company and of the processing to be carried out by the Company, as detailed in this Data Privacy Notice.

6. WHAT ARE THE PURPOSES FOR WHICH DATA IS PROCESSED AND WHAT IS OUR LEGAL BASIS FOR CARRYING OUT THE PROCESSING?²

- 6.1 Your personal data is collected and processed for various business purposes, in accordance with applicable laws. We have set out in this Data Privacy Notice the purposes we may use your personal data for. Data may occasionally be used for purposes not obvious to you where the circumstances warrant such use (e.g. in investigations or disciplinary proceedings). We may, where we think it is necessary, provide you with additional information in relevant People policies to ensure that you understand how your personal data may be used.

6.2 The legal basis on which we process your personal data

- 6.2.1 Whenever the Company processes your personal data we do so on the basis of a legal basis or justification for that processing. Processing of special categories of data is always justified on the basis of an additional lawful condition. In the majority of cases, the processing of your personal data will be justified on one of the following basis:

6.2.1.1 The processing is necessary for compliance with a legal obligation to which the Company is subject (e.g. disclosing information to HMRC, making statutory payments, avoiding unlawful termination, avoiding unlawful discrimination or health and safety obligations); or

6.2.1.2 Where there is no legal obligation we will process your data where the processing is necessary for the performance of a contract to which you are a party to in order to take steps at your request prior to entering into such a contract (e.g. collecting bank details to pay your salary);

6.2.1.3 Where the above two grounds do not apply we may process your personal data where the processing is necessary for the legitimate interests pursued by the Company, except where such interests are overridden by your interests or fundamental rights and freedoms which require protection of personal data. The Company considers that it has a legitimate interest in processing data for the purposes set out above. This is necessary to ensure fair and effective recruitment of suitable colleagues and the effective reward, administration, support, development and management of colleagues. This is important to ensure that the Company continues to meet its business objectives and goals both in the short and long term; maintains its reputation; and continues to attract and retain high calibre colleagues.

- 6.2.2 We may on occasion process your personal data for the purpose of legitimate interests pursued by a third party, except where such interests are overridden by your interests or fundamental rights and freedoms which require protection of personal data (e.g. to meet the security requirements of our Business Partners).

- 6.2.3 In exceptional circumstances where we have no legitimate interest in processing but you ask us to process data for a particular purpose we may carry out the processing on the basis of your consent (e.g. if you ask us to provide pay information to a bank for a mortgage application made by you). Where we rely on this we will make this clear at the time.

- 6.2.4 We have set out in [Appendix 1](#) the purposes we may use your personal data for and the legal basis we rely on in each case.

6.3 **Additional legal basis we rely on where we process special category data**

The special categories of personal data that may be processed by the Company are set out in [Appendix 2](#). Where we process special categories of data it will be justified by a condition set out at 6.2.1 above and also by one of the following additional conditions:

- 6.3.1 The processing is necessary for the purposes of carrying out the obligations and exercising the rights of you or the Company in the field of employment law, social security and social protection law, to the extent permissible under applicable laws;
- 6.3.2 The processing is necessary for the purposes of occupational medicine, for the assessment of your working ability and medical diagnosis, to the extent permitted by applicable laws;
- 6.3.3 The processing is necessary to protect your vital interests or of another person where you are physically or legally incapable of giving consent (e.g. in a medical emergency);
- 6.3.4 The processing is necessary for purposes authorised by applicable law. This includes:
 - 6.3.4.1 Data Protection Bill 2018
- 6.3.5 The processing is necessary for the establishment, exercise or defence of legal claims; or
- 6.3.6 In exceptional circumstances the processing is carried out subject to your explicit consent (as explained in Appendix 2).

6.4 **Processing data relating to criminal convictions and offences**

Personal data relating to criminal convictions and offences will only be processed where authorised by applicable laws e.g:

- 6.4.1 a criminal record check may be carried out on recruitment or transfer or intermittently where ongoing screening is required where authorised by applicable laws; or
- 6.4.2 an allegation of a criminal offence or conviction arising during your relationship with the Company may be processed where required or authorised by applicable law e.g:
 - 6.4.2.1 where we have a legal or regulatory requirement to report an offence; or
 - 6.4.2.2 applicable laws authorise the Company to process information about the offence (e.g. in a disciplinary process) for the purpose of making decisions regarding your relationship with the Company.

7. **AUTOMATED DECISION MAKING AND PROFILING**

- 7.1 We do not currently rely on automated decision making.

8. **RETENTION OF PERSONAL DATA**

- 8.1 The Company strives to ensure that personal data are kept as current as possible and that irrelevant or excessive data are deleted or made anonymous as soon as reasonably practicable.
- 8.2 We generally retain personal data for as long as is required to satisfy the purpose for which it was collected. This will usually be the period of your employment/contract with us plus the length of any applicable statutory limitation period following your departure, although some data, such as pension information, may need to be kept for longer. We may keep some specific types of data e.g. tax records, for different periods of time, as required by applicable law. However, some personal data may be retained for varying time periods in order to fulfil any legal and regulatory obligations and for other legitimate business reasons. Please see the Company's Data Retention Policy for further information.

9. DISCLOSURES OF PERSONAL DATA

- 9.1 Within the Company, your personal data can be accessed by or may be disclosed internally on a need-to-know basis to:
- 9.1.1 local, regional and global People team, including managers and team members;
 - 9.1.2 local, regional and executive management responsible for managing or making decisions in connection with your relationship with the Company or when involved in an People process concerning your relationship with the Company;
 - 9.1.3 system administrators; and
 - 9.1.4 where necessary for the performance of specific tasks or system maintenance by staff in the Company teams such as the Finance and CPP Tech and the Global People team.
- 9.2 Certain basic personal data, such as your name, location, job title, contact information, colleague number and any published skills and experience profile may also be accessible to other colleagues. The security measures in place within the Company to protect your data are set out below.
- 9.3 Your personal data may also be accessed by third parties whom we work together with.
- 9.4 Personal data may also be shared with certain interconnecting systems such as the main People system and local payroll and benefits systems. Data contained in such systems may be accessible by providers of those systems, their associated companies and sub-contractors.
- 9.5 Examples of third parties with whom your data will be shared include tax authorities, regulatory authorities, the Company's insurers, IT administrators, lawyers, auditors, investors, consultants and other professional advisors, payroll providers, and administrators of the Company's benefits programs. The Company expects such third parties to process any data disclosed to them in accordance with applicable law, including with respect to data confidentiality and security.
- 9.6 Where these third parties act as a "data processor" (e.g. a payroll provider) they carry out their tasks on our behalf and upon our instructions for the above mentioned purposes. In this case your personal data will only be disclosed to these parties to the extent necessary to provide the required services.
- 9.7 In addition, we may share personal data with national authorities in order to fulfil a legal obligation to which we are subject e.g. the case in the framework of imminent or pending legal proceedings or a statutory audit.
- 9.8 Under our regulatory obligation, we have a requirement to share some aspects of your personal data with the FCA [name, job title, accredited body membership, qualifications, employment dates, workplace location, date of birth, social security number]. This will be only be done when we have undertaken any disciplinary action with you and where conduct rules were breached to cause the disciplinary action to be required. Please note that disciplinary action has to result in one or more of the following for it to be reportable to the FCA under a conduct rule breach: 1. Issuing a formal written warning 2. Dismissal of that person 3. Reducing or recovering any of your remuneration.

10. SECURITY OF DATA

- 10.1 The Company is committed to protecting the security of the personal data you share with us.

11. INTERNATIONAL TRANSFER OF PERSONAL DATA

- 11.1 The Company does not send your data outside of the European Economic Area (EEA). However if there was an exceptional requirement to send any of your data to a country outside of the EEA the Company would ensure that the country to which the data was being sent either had adequate

provisions for processing and managing your data or demonstrated the same level of privacy protocols required by those countries in the EEA.

12. YOUR RIGHTS AS A DATA SUBJECT

12.1 Right to access, correct and delete your personal data

12.1.1 The Company aims to ensure that all personal data are correct. You also have a responsibility to ensure that changes in personal circumstances (e.g. change of address and bank accounts) are notified to the Company so that we can ensure that your data is up-to-date.

12.1.2 You have the right to request access to any of your personal data that the Company may hold, and to request correction of any inaccurate data relating to you. In addition you have the right to request the deletion of any irrelevant data we hold about you.

12.1.3 You can see and update some of this data yourself via Cascade (People system). However, to correct/update other information, you will need to contact your local People team.

12.2 Data portability

Where we are relying upon your consent or the fact that the processing is necessary for the performance of a contract to which you are party as the legal basis for processing, and that personal data is processed by automatic means, you have the right to receive all such personal data which you have provided to the Company in a structured, commonly used and machine-readable format, and also to require us to transmit it to another controller where this is technically feasible.

12.3 Right to restriction of processing:

You have the right to restrict our processing of your personal data where:

12.3.1 you contest the accuracy of the personal data until we have taken sufficient steps to correct or verify its accuracy;

12.3.2 where the processing is unlawful but you do not want us to erase the data;

12.3.3 where we no longer need the personal data for the purposes of the processing, but you require them for the establishment, exercise or defence of legal claims; or

12.3.4 where you have objected to processing justified on legitimate interest grounds (see below) pending verification as to whether the Company has compelling legitimate grounds to continue processing.

Where personal data is subjected to restriction in this way we will only process it with your consent or for the establishment, exercise or defence of legal claims.

12.4 Right to withdraw consent

Where we have relied on your consent to process particular information and you have provided us with your consent to process data, you have the right to withdraw such consent at any time. You can do this by (i) in some cases deleting the relevant data from Cascade (although note that in this case it may remain in back-ups and linked systems until it is deleted in accordance with our data retention policy) or (ii) contacting your local People contact. It will only however be rarely that we rely on your consent to process personal data for your employment or engagement.

12.5 Right to object to processing justified on legitimate interest grounds

Where we are relying upon legitimate interest to process data, then you have the right to object to that processing. If you object, we must stop that processing unless we can either demonstrate compelling legitimate grounds for the processing that override your interests, rights and freedoms or where we need to process the data for the establishment, exercise or defence of legal claims. Where

we rely upon legitimate interest as a basis for processing we believe that we can demonstrate such compelling legitimate grounds, but we will consider each case on an individual basis.

12.6 **Right to complain**

You also have the right to lodge a complaint with the relevant authority if you consider that the processing of your personal data infringes applicable law.

12.7 For further information regarding your rights, or to exercise any of your rights, please contact dataprivacy@cpp.co.uk