DATA PROTECTION POLICY DOCUMENT and PRIVACY NOTICE

OCTOBER 2018

1. INTRODUCTION

1.1 This Data Protection Policy sets out how Corporate Architecture Limited ("we", "the Company") handle the Personal Data of our customers, suppliers, employees, workers and other third parties.

1.2 This policy applies to educate staff on how to Process Personal Data of customers, clients or (in limited circumstances) other colleagues, in accordance with the General Data Protection Regulations ('GDPR').

1.3 The second part of this policy is a Privacy Notice, which has also been drafted to set out what Personal Data the Company Processes about you and all other staff, what Personal Data we may need to Process in future, and your rights in relation to how the Company uses that data.

1.4 This policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

1.5 This policy and the Privacy Notice applies to all staff, including all employees, workers, contractors, agency workers, consultants, directors, members and others. You must read, understand and comply with this policy when Processing Personal Data on our behalf and attend training on its requirements. This policy sets out what we expect from you in order for the Company to comply with applicable law and compliance with its rules is mandatory.

1.6 This policy is pervasive in nature, and our other policies may be updated in order to be compliant with the GDPR. You must also comply with all such related policies, notices and guidelines, issued and updated from time to time. Any breach of this policy or the Privacy Notice (or any other policy), resulting in actual or potential risk of liability for the Company may result in disciplinary action.

1.7 This policy and the Privacy Notice is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the DPO.

1.8 We will train staff on the GDPR and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. Any updates will be briefed at staff meetings. The Company is obliged to maintain a record of training attendance by Company Personnel.

1.9 We will also regularly test, using a checklist, the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

1.10 All staff will receive training on this policy and the content of the Privacy Notice. Staff who are required to process Personal Data as part of their day to day activities will receive additional training on GDPR compliance, tailored to their role.

2. DEFINITIONS

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Company name: Corporate Architecture Limited

Consent: freely given, specific, informed and unambiguous agreement by the Data Subject.

Data Controller: Corporate Architecture Limited are the Data Controller of all Personal Data relating to our staff and clients, which is used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity.

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under the GDPR.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

Personal Data: any information identifying a Data Subject (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises or is likely to compromise the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when the Company collects information about them.

Processing or Process: any activity that involves the use of Personal Data, including obtaining, recording or holding the data, organising, amending, retrieving, using, disclosing, erasing or destroying it and transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

3. RESPONSIBILITY FOR POLICY

3.1 We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times.

3.2 The Company is exposed to potential fines of up to EUR20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

3.3 All departments, members of management, Directors and staff are responsible for ensuring all Company Personnel comply with this policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

3.4 The DPO is responsible for overseeing this policy. This post is held by Charlie Drucquer, Design Studio Manager, *support@corporatearchitecture.co.uk*.

4. WHEN TO CONTACT THE DPO

4.1 The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

4.2 If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPO. You should preserve all evidence relating to the potential Personal Data Breach.

4.3 You may also contact the DPO with any questions about the operation of this policy, other related policies, or the GDPR, or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

(a) if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Company);

(b) if you need to rely on Consent and/or need to capture Explicit Consent;

(c) if you need to draft Privacy Notices or Fair Processing Notices;

(d) if you are unsure about the retention period for the Personal Data being Processed;

(e) if you are unsure about what security or other measures you need to implement to protect Personal Data;

(f) if there has been a Personal Data Breach;

(g) if you are unsure on what basis to transfer Personal Data outside the EEA;

(h) if you need any assistance dealing with any rights invoked by a Data Subject;

(i) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA, or otherwise plan to use Personal Data for purposes others than what it was collected for;

(j) if you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making;

(k) if you are authorised to make posts on social media on behalf of the Company, and that post will involve Processing Personal Data;

(l) if you need help complying with applicable law when carrying out direct marketing activities; or

(m) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors).

You must comply with the Company's guidelines on DPIA and Privacy by Design, which may be required to be implemented by the DPO, from time to time.

5. DIRECT MARKETING

5.1 Whilst we carry out limited marketing activities, we are subject to certain rules and privacy laws when marketing to our customers.

5.2 For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

5.3 The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

5.4 A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

5.5 Any issues with direct marketing to Data Subjects, or requests for suppression must be passed to the DPO.

6. SHARING PERSONAL DATA

6.1 Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

6.2 You may only share the Personal Data we hold with another employee, agent or representative of Corporate Architecture Limited if the recipient has a job-related need to know the information. Alternatively, we may be required to disclose Personal Data of individual Data Subjects as part of planning or other property applications, where named individuals need to be identified.

6.3 You may only share the Personal Data we hold with third parties, such as our service providers, or Councils and as part of planning or other applications if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(d) the transfer complies with any applicable cross border transfer restrictions; and

(e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

6.4 You must comply with the Company's guidelines on sharing data with third parties. We may also be obliged to comply with more stringent contractual obligations owed to clients not to disclose any information about the services we provide to them.

6.5 Data subjects must make a formal request for information we hold about them, or to exercise other rights in relation to their data. All such communications must be made in writing. Employees who receive a written request should forward it to the DPO immediately.

6.6 When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

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

(b) We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

6.7 Staff should refer any requests related to the GDPR to the DPO for assistance in difficult situations. Employees should not be bullied into disclosing Personal Data.

7. DATA SECURITY

7.1 All staff are responsible for ensuring the security of any Personal Data or Sensitive Personal Data held by the Company about Data Subjects.

7.2 Personal Data, including different categories and sub-sets of Personal Data will only be processed by a limited number of staff, where it is directly relevant to their duties. For example, the Accounts Team may have access to staff bank account details, to process payroll. Security steps will be taken to limit access by any other staff to this information.

7.3 Personal Data will be stored safely and securely, whether held in paper or electronic form. Physical areas of Company premises may have access restricted to ensure the security of Personal Data. Equally, electronic documentation, databases or other means of electronically storing Personal Data may be encrypted, password protected, or require other security measures to be implemented, to restrict access and maintain confidentiality.

7.4 Our range of security measures to keep hard copy and electronic data and cloud data secure include:

(a) **Entry controls**. Any stranger seen in entry-controlled areas should be reported.

(b) **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.) Staff should operate a clean desk policy of tidying away documents from their desk, and locking this in a filing cabinet, desk drawer or cupboard.

(c) **Methods of disposal.** Paper documents should be shredded in the shredding bins provided. Confidential documents, containing Personal Data should not be placed in general waste bins. Digital storage devices should have any data wiped, and be physically destroyed when they are no longer required.

(d) **Password Protection**. Passwords should not be shared between staff, to ensure access to Personal Data is limited to core staff only.

(e) **Virus Protection**. Ensure any Company devices receive and complete all updates to maintain the effectiveness of our online security systems.

7.5 Other security measures staff are required to take to keep data secure include:

(a) Data users must ensure that individual monitors do not show confidential information and/or Personal Data to passers-by and that they log off from their PC when it is left unattended.

(b) Staff should not use Company equipment to process Personal Data of staff, clients or other third parties in public, or where there is a risk that unauthorised people may view or access Personal Data and/or confidential information. For example, staff should not use devices to process Personal Data on trains or cafés, where there screen can be overlooked.

(c) Staff should not use Company or personal equipment or devices to access unsecured public Wifi connections, when processing Personal Data and/or using confidential information.

(d) Any staff required to work from home, when processing Personal Data or confidential information should use Company equipment, which is secure and protected from viruses and other online threats. Devices and hard copy records containing Personal Data, Sensitive Personal Data or confidential information should be stored securely when not in use, to prevent unauthorised access by family members or any other third parties. Personal Data of staff, clients or other third parties should never be accessed or otherwise Processed on a personal device.

(e) Staff should not under any circumstances leave Company devices, equipment or hard copy Personal Data or confidential information unsupervised in a public place, including but not limited to on public transport, or any other vehicle.

(f) Staff using Company devices should ensure that all software updates are completed, to ensure that virus protection, firewall and other protective security software is up to date.

(g) Staff are not permitted to use memory sticks for storage of Personal Data.

9. EXAMPLES OF POTENTIAL PERSONAL DATA BREACHES AND/OR BREACHES OF THIS POLICY

9.1 Unauthorised disclosure of Personal Data to a third party without any justification, consent, or authorisation.

9.2 Failure to contact the DPO when required, on any Data Protection matter.

9.3 Unauthorised disclosure of Personal Data about a client, third party, or colleague in an inappropriate forum, including but not limited to social media posts, email correspondence or telephone conversations.

9.4 Unauthorised disclosure of Personal Data to a colleague, where that colleague has no access to that Personal Data, and no work-related need or justification to access that Personal Data.

9.5 Failure to carry out identity checks before disclosure of Personal Data.

9.6 Undertaking unauthorised Processing without informing a Data Subject.

9.7 Unauthorised Processing of Personal Data on a personal device, on an unsecured wireless network, or on any other platform which jeopardises or risks jeopardising the security of that Personal Data.

9.8 Loss of Personal Data for any reason.

This list is not exhaustive.

STAFF PRIVACY NOTICE

1. PERSONAL DATA PROTECTION PRINCIPLES

1.1 When processing the Personal Data of staff, clients or any other Data Subjects, we adhere to the principles set out in the GDPR which require Personal Data to be:

(a) **Processed lawfully, fairly and in a transparent manner**.
Purposes the Company may use when processing staff, client or third party Personal Data include where the Data Subject has given Consent, the processing is necessary for the performance of a contract with the Data Subject, to meet legal compliance obligations, to protect the Data Subject's vital interests, and to pursue the Company's legitimate business interests.
We must identify and document the legal ground relied on for each processing activity. Further details about the grounds are set out in Schedule 1.

(b) **Collected only for specified, explicit and legitimate purposes (Purpose Limitation).**
Personal Data cannot be used for new different, or incompatible purposes which were not disclosed when the Personal Data was obtained. You may need to inform the Data Subject of any new usage of their Personal Data, and may need to seek their Consent before Processing.

(c) **Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).**
We may only collect and process Personal Data required for our purposes and your job duties. We must not collect or process excessive or irrelevant Personal Data.

(d) **Accurate and where necessary kept up to date (Accuracy).**
The accuracy of Personal Data must be checked and the point of collection and at regular intervals afterwards. All reasonable steps must be taken to amend or securely destroy inaccurate or out of date Personal Data.
You have a duty to notify us of any changes to your Personal Data, as soon as possible.

(e) **Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).**
Personal Data which is no longer required, must be securely destroyed or erased from our systems. This includes requiring third parties to delete such data where applicable.
We have different retention periods for different kinds of Personal Data, set out at Schedule 1.

(f) **Processed in a manner that ensures its security (Security, Integrity and Confidentiality).**
Personal Data must be secured using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage.
Particular care must be taken in protecting Sensitive Personal Data, and third party service providers must also comply with security measures to protect Personal Data, before any transfer is made.

(g) **Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).**
Data transfers to countries outside of the EEA is restricted, unless appropriate conditions are met. Personal Data will be transferred across borders, when you transmit, send, view or otherwise access data in or send it to, a different country.
We have an operation based in the US, and we anticipate that some Personal Data will be transferred to this business for the purposes of bonus payments. We must still ensure that countries both within and outside the EEA are compliant with the General Data Protection Regulation. The US is currently recognised by the European Commission has having adequate protections in place to be compliant with GDPR.

(h) **Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).**
These are listed in full at paragraph 2. You may exercise your rights in accordance with paragraph 3.

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

2. DATA SUBJECT'S RIGHTS

2.1 All Data Subjects, including you, other staff and clients have rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw Consent to Processing at any time;

(b) receive certain information about the Data Controller's Processing activities;

(c) request access to their Personal Data that we hold;

(d) prevent our use of their Personal Data for direct marketing purposes;

(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

(f) restrict Processing in specific circumstances;

(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;

(i) object to decisions based solely on Automated Processing, including profiling (ADM);

(j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(l) make a complaint to the supervisory authority. (Data Subjects have the right to make a complaint at any time to the Information Commissioner's Office (ICO)); and

(m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

2.2 You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

2.3 We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

3. DATA SUBJECT REQUESTS

3.1 If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, request that we transfer a copy of your personal information to another party, withdraw your Consent to processing, or otherwise exercise any of your GDPR rights, please contact the DPO in writing.

3.2 You must immediately forward any Data Subject request you receive to the DPO.

3.3 Any written application to the DPO must explicitly identify which right(s) you wish to exercise, from the following options:

(a) **Request access to your personal information** (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

(b) **Request correction of the personal information** that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

(c) **Request erasure of your personal information**. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing.

(d) **Object to processing of your personal information** where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

(e) **Request the restriction of processing of your personal information.** This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

(f) **Request the transfer of your personal information to another party.**

(g) **Withdraw Consent to processing of your personal information.**

3.4 You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

3.5 The Company is required to respond to any Data Subject Requests within one month of the date of the request. Where we cannot meet this deadline, we will inform you of our reasons for any delay in writing, and extend the response period to two months.

3.6 In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your Personal Data for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the DPO.

3.7 Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

3.8 If you are unsatisfied with the manner in which we have dealt with your Data Subject Request, you may make a complaint to the Information Commissioner.

4. WHAT PERSONAL DATA DO WE HOLD ABOUT YOU?

4.1 We will collect, store, and use the following categories of personal information about you:

(a) Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.

(b) Date of birth.

(c) Gender.

(d) Marital status and dependants.

(e) Next of kin and emergency contact information.

(f) National Insurance number.

(g) Bank account details, payroll records and tax status information.

(h) Salary, annual leave, pension and benefits information.

(i) Start date.

(j) Location of employment or workplace.

(k) Copy of driving licence.

(l) Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).

(m) Employment records (including job titles, work history, working hours, induction and training records and professional memberships).

(n) Compensation history.

(o) Performance information.

(p) Disciplinary and grievance information, (including evidence gathered as part of an investigation, and any related sanctions or outcomes).

(q) CCTV footage and other information obtained through electronic means such as premises access records.

(r) Information about your use of our information and communications systems.

(s) Photographs.

(t) Health and Safety Information (including risk assessments, accident book records, medical records).

(u) Mobile phone data (including location data, phone usage, call logs).

(v) Email records (in the event you elect to use your work email for personal matters).

(w) References, whether produced by us, or provided by third parties.

(x) Meeting minutes (for example, for disciplinary hearings, grievance meetings, performance management meetings, exit interviews).

4.2 We may also collect, store and use the following "special categories" of more sensitive personal information:

(a) Information about your health, including any medical condition, health and sickness records, fit notes, or reports produced by a GP or Consultant treating you.

(b) Biometric data, for example (laptop and phone access).

(c) Information about criminal convictions and offences (for example through voluntary disclosure).

We will seek your explicit consent before Processing any Sensitive Personal Data

5. HOW IS YOUR PERSONAL INFORMATION COLLECTED?

5.1 We collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, or other background check agencies.

5.2 We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

6. HOW WE WILL USE INFORMATION ABOUT YOU

6.1 We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

(a) Where we need to perform the contract we have entered into with you (for example, to use bank account details to pay you).

(b) Where we need to comply with a legal obligation (such as our obligation to provide a safe place of work, or disclose criminal activity to a third party such as the Police).

(c) Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

6.2 We may also use your personal information in the following situations, which are likely to be rare:

(a) Where we need to protect your interests (or someone else's interests).

(b) Where it is needed in the public interest or for official purposes.

7. SITUATIONS IN WHICH WE WILL USE YOUR PERSONAL INFORMATION

7.1 We need all the categories of information in the list above (see paragraph 4) primarily to allow us to perform our contract with you and to enable us to comply with legal obligations.

7.2 In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below.

(a) Making a decision about your recruitment or appointment.

(b) Determining the terms on which you work for us.

(c) Checking you are legally entitled to work in the UK.

(d) Paying you and, if you are an employee, deducting tax and National Insurance contributions.

(e) Requesting references from your previous employer, or providing references on your behalf.

(f) Providing the following benefits to you: Life Assurance, Private Medical Insurance and Group Income Protection.

(g) Liaising with your pension provider.

(h) Administering the contract we have entered into with you.

(i) Making immigration applications, bookings and travel arrangements on your behalf for travel on Company business.

(j) Business management and planning, including accounting and auditing.

(k) Conducting performance reviews, managing performance, determining performance requirements, conducting exit interviews.

(l) Making decisions about salary reviews and compensation.

(m) Assessing qualifications for a particular job or task, including decisions about promotions.

(n) Gathering evidence for use in possible grievance or disciplinary hearings.

(o) For monitoring the number and identity of staff working or otherwise present on site.

(p) To ensure the security of our premises.

(q) To ensure you are driving Company vehicles in an authorised manner, in accordance with the Highway Code and road traffic regulations.

(r) Making decisions about your continued employment or engagement.

(s) Making arrangements for the termination of our working relationship.

(t) Education, training and development requirements.

(u) Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.

(v) Ascertaining your fitness to work.

(w) Managing sickness absence.

(x) Complying with health and safety obligations.

(y) To prevent fraud.

(z) To monitor your use of our information and communication systems to ensure compliance with our IT policies.

(aa) To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.

(bb) Equal opportunities monitoring.

7.3 Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

7.4 If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

8. CHANGE OF PURPOSE

8.1 We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

8.2 Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

9. PROCESSING AND TRANSFERRING DATA WITHIN and OUTSIDE OF THE EEA

9.1 The Company work for clients who have international interests It may be necessary to Process Personal Data and Sensitive Personal Data about individual clients, staff and third parties both within and across the UK and other jurisdictions in the course of our business operations, or for the performance of the employment contract with you.

9.2 In particular, we may need to Process and disclose Personal Data and Sensitive Personal Data about you in the course of making VISA applications, and making flight and accommodation bookings for you to travel on Company business. We must still ensure that countries and third parties both within and outside the EEA are compliant with the General Data Protection Regulation.

9.3 However, to ensure that the Personal Data of our clients and other individuals does receive an adequate level of protection we have put in place the following appropriate measures to ensure that your Personal Data is treated by those third parties in a way that is consistent with and which respects the EU and UK laws on data protection:

(a) binding corporate rules (agreements governing transfers made between organisations within in a corporate group);

(b) contractual clauses agreed authorised by the competent supervisory authority; or

9.4 If you require further information about these protective measures, you can request it from Human Resources.

9.5 You may transfer Personal Data of a third party where the organisation receiving the Personal Data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer.

9.6 You should contact the DPO before any Personal Data is Processed or transferred to a new jurisdiction where we do not operate. If you have any queries about safeguards to be taken when transferring Personal Data, please also contact the DPO.

10. HOW WE USE SENSITIVE PERSONAL INFORMATION

10.1 "Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

(a) In limited circumstances, with your explicit written consent.

(b) Where we need to carry out our legal obligations and in line with our legal obligations.

(c) Where it is needed in the public interest, such as for equal opportunities monitoring.

(d) Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

10.2 Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about staff members or former staff members in the course of legitimate business activities with the appropriate safeguards.

11. OUR OBLIGATIONS AS AN EMPLOYER

11.1 We will use your particularly sensitive personal information in the following ways:

11.2 We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.

11.3 We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence, to take legal advice on our obligations to you and to administer benefits.

11.4 We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

12. YOUR OBLIGATIONS TO US

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

13. DO WE NEED YOUR CONSENT?

13.1 We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law.

13.2 In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. For example, consent to use your biometric data to access our electronic devices

13.3 If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

14. INFORMATION ABOUT CRIMINAL CONVICTIONS

14.1 We will only collect information about criminal convictions if they are voluntarily disclosed by you, we have your consent to consider the information, and it is appropriate given the nature of the role. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us.

14.2 Any disclosure of a criminal conviction will be Processed in accordance with the principles set out at clause 1.

15. CONFIDENTIALITY

15.1 You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data (whether of staff or clients), defined as follows:

(a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.

(b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.

(c) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

16. SHARING EMPLOYEE PERSONAL DATA

16.1 We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

16.2 We may have to share your data with third parties, including third-party service providers such as BUPA. We require third parties to respect the security of your data and to treat it in accordance with the law.

16.3 "Third parties" includes third-party service providers (including contractors and designated agents) and other entities within our group. The following activities are carried out by third-party service providers: payroll, pension administration, benefits provision and administration, IT services and BUPA.

16.4 Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

16.5 We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained from Human Resources.

16.6 All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

16.7 We may transfer your personal information outside the EU. If we do, you can expect a similar degree of protection in respect of your personal information.

16.8 We will share your personal information with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data and for the purpose of Bonuses and Insurances.

16.9 We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. We may also need to share your personal information with a regulator, for the purposes of seeking legal advice, or to otherwise comply with the law.

16.10 We may also have additional legal justifications or statutory obligations to share Personal Data with third parties. For example, we may need to disclose Personal Data to the Police (in the event of actual or suspected criminal activity) a professional regulator (in the event of any professional misconduct), or the Jobcentre (for the purposes of processing any application for benefits).

17. AUTOMATED PROCESSING (INCLUDING PROFILING) AND AUTOMATED DECISION-MAKING

17.1 We do not use Automated Processing or Automated Decision-Making in our business to process Personal Data or Sensitive Personal Data of staff, clients or third parties.

17.2 We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

18. DATA SECURITY

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

19. DATA RETENTION

19.1 We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are available in the chart at the end of this policy.

19.2 To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, any legal obligations or justifications to retain data, and the applicable legal requirements.

19.3 In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

19.4 Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information. We may ask for your consent to retain some of your information for the purposes of giving references.

20. CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update our policies, or this Privacy Notice at any time, and we will provide you with a new policy when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

21. ACKNOWLEDGMENT

I, _____, acknowledge that on _____[DATE], I received and read a copy of Corporate Architecture Limited's Data Protection Policy and Privacy Notice dated October 2018 and understand that I am responsible for knowing and abiding by its terms.

I understand that the information in this policy is intended to help Company staff to work together effectively on assigned job responsibilities and assist in the use and protection of Personal Data. This policy does not set terms or conditions of employment or form part of an employment contract.

Signed ……

Printed Name ……

Date ……

SCHEDULE 1

Categories of Personal Data/Sensitive Personal Data	Recipients of the Personal Data/Sensitive Personal Data	Justification for processing the Personal Data/Sensitive Personal Data	Retention Periods
CV/Covering Letter, Application forms Notes of recruitment process and decisions made.	Management Team Human Resources	For the performance of an eventual employment contract. Consent will be sought from all applicants at submission stage to Process their application. Complying with a legal obligation (Equality Act 2010, discrimination in recruitment).	For unsuccessful job applicants, twelve months after the recruitment process. For successful applicants, the duration of your employment and seven years after termination of your employment. (Limitation period of civil breach of contract claims.)
Name, address, telephone number, personal email address, start date, location of workplace, date of birth, next of kin emergency contact information.	Management Team Human Resources External Payroll	For the performance of your contract. For example, determining eligibility for and processing staff benefits (such as pension payments), or contacting you about employment changes. To protect the vital interests of the Data Subject. For example, contacting their next of kin in the event of an emergency.	From the recruitment process, throughout your employment. Next of kin contact information will be deleted on termination of employment. Name and contact details will be retained for seven years after termination of employment, with consent for the purpose of giving references.
Copy of passport and any other immigration documents.	Management Team Human Resources International immigration services. Service providers abroad.	Legal obligation, under the Immigration, Asylum and Nationality Act 2006 and the Immigration Act 2014. To ensure your right to work in the UK. This documentation may be inspected from time to time by an immigration officer, as part of an inspection. For the Company's vital interests, to make travel bookings to enable you to go abroad in the course of your duties.	Will be updated periodically throughout your employment. Seven years after termination of employment, in case of immigration enforcement action.

National Insurance number, payroll records and tax status information.	Management Team Human Resources HMRC External Payroll	Legal obligation to comply with payroll reporting to HMRC. Identifiable information about your gender and pay may be used for producing anonymous calculations to comply with gender pay gap reporting requirements (Equality Act 2010). Performance of your employment contract, to pay you.	The duration of your employment. Seven years after termination of employment, for compliance with potential future HMRC audit.
Bank Details	Management Team Accounts Human Resources External Payroll	Performance of your employment contract, to pay you.	The duration of your employment. Retained until final payments made to you on or after termination of your employment.
Bonus and Pay Reviews	Management Team Human Resources	Performance of your employment contract, to pay you.	Will be updated periodically throughout your employment. Seven years after termination of employment. (The limitation period for breach of contract claims.)
Pension Scheme and Employee Benefit Schemes	Management Team Human Resources BUPA Insurance Broker Peoples Pension. External Payroll	Performance of your employment contract, for contractual benefits to be processed.	The duration of your employment. Seven years after termination of employment. (The limitation period for breach of contract claims.)
Holiday records	Management Team Human Resources Staff teams	Legal obligation to provide holiday under the Working Time Regulations 1998. Performance of your employment contract, for contractual benefits to be processed. Pursuing the legitimate interests of the Data Controller, to manage staff leave and availability fairly.	The duration of your employment. Seven years after termination of employment. (The limitation period for breach of contract claims.)

Absence Records (Sickness, compassionate leave, jury service, volunteer reservists, or any other absence)	Management Team Human Resources External Payroll	Pursuing the legitimate interests of the Data Controller. Performance of Employment Contract. (recording reasons for absence when staff member unable to perform their duties under the contract of employment, facilitate payment).	Seven years after termination of employment. (The limitation period for breach of contract claims.)
Expenses Records Company Credit Card Records	Accounts Management Team External Payroll Human Resources	Pursuing the legitimate interests of the Data Controller, to monitor spending for Company purposes.	Seven years from end of financial year in which expense occurred, for compliance with potential future HMRC audit
Driving Licence Information, Vehicle Insurance Policy and MOT Certificate	Management Team Human Resources External Payroll Insurance Broker Third Party Insurance Provider,	Legal obligation to ensure staff driving on Company business are legally qualified to do so, and are in a safe vehicle. In compliance with legal obligations and guidance in the Highway Code and our health and safety obligations.	Three years after termination of employment. (The limitation period for personal injury claims.)
References given by past Employer	Management Team Human Resources	Performance of employment contract. To ensure the suitability of the person appointed to a role.	Seven years after your appointment. (The limitation period for civil claims.)
Contract of Employment Variations to Contract (Promotions, pay rises, changes to terms)	Management Team Human Resources	Performance of Employment Contract. Pursuing the legitimate interests of the Data Controller (their respective contractual rights).	The duration of your employment. Seven years after termination of employment. (The limitation period for civil breach of contract claims.)

Premises Access Logs (Employee sign in book)	Management Team Human Resources	Pursuing the legitimate interests of the Data Controller, to control access to their premises, to ensure the health and safety of staff and visitors, ensure compliance with rules, to pursue disciplinary action. To protect the vital interests of the Data Subject, ensuring their health and safety on the premises.	For six months, for the safety and security of company premises. This footage may be used as part of the disciplinary procedure.
Training Records/ Appraisal Records	Management Team	Performance of the contract with the Data Subject. To ensure that the data subject is discharging their duties.	For the duration of your employment and twelve months after termination. (The limitation period for employment tribunal claims.)
Flexible Working Requests (Requests, Meeting Minutes, Outcome Letters, Appeal correspondence, Variation to Contract documents)	Management Team Human Resources External Payroll	In accordance with a legal obligation, for the Data Subject, to ensure they can exercise a statutory right (Employment Rights Act 1996). For performance of the employment contract.	For the duration of your employment and twelve months after termination. (The limitation period for employment tribunal claims.)
CCTV footage	Management Team External IT	Pursuing the legitimate interests of the Data Controller, to control access to their premises, to ensure the health and safety of staff and visitors, ensure compliance with rules, to pursue disciplinary action. To protect the vital interests of the Data Subject, ensuring their health and safety on the premises.	For six months, for the safety and security of company premises. This footage may be used as part of the disciplinary procedure. In certain circumstances, CCTV footage may need to be disclosed to the Police for the prevention or detection of crime.

Medical Records, Medical Reports, Health Checks, Sickness Absence Record, Fit Notes, Self-certification, Capability Procedures, BUPA application.	Management Team Human Resources Insurance Broker BUPA	Compliance with a legal obligation, to provide a safe system of work for the Data Subject, and/or for the purposes of making reasonable adjustments in accordance with our obligations under the Equality Act 2010. In accordance with the contract of employment, to give contractual benefits. With the Consent of the Data Subject.	The duration of your employment and up to three years after termination. In the event that there is a risk of a latent personal injury claim, relevant medical evidence may be preserved for longer, in accordance with our obligation to preserve evidence for litigation.
Biometric Information Fingerprint access for mobile phones.	IT Manager	Consent of the Data Subject. Pursuing the legitimate interests of the Data Controller, for security of equipment and data.	The duration of employment.
Family Leave Requests (Maternity, Paternity, Adoption, Parental or Shared Parental Leave Requests)	Management Team Human Resources	In accordance with a legal obligation, for the Data Subject to exercise statutory rights to family leave and pay. For the performance of the employment contract.	For the duration of your employment and twelve months after termination. (The limitation period for employment tribunal claims.)
Health and Safety Information (Accident Book Records, Risk Assessments, Desk Assessments, Display Screen Equipment assessments and contributions to cost of glasses.)	Management Team Human Resources Health and Safety Representatives Health and Safety Consultant.	Pursuing the legitimate interests of the Data Controller, for the prevention and detection of accidents, evaluation of risk, to ensure the health and safety of staff and visitors, ensure compliance with rules, to pursue disciplinary action. To protect the vital interests of the Data Subject, ensuring their health and safety on the premises. To comply with the legal obligation to provide a safe system of work.	The duration of the Data Subject's employment and up to three years after termination. In the event that there is a risk of a latent personal injury claim, relevant medical evidence may be preserved for longer, in accordance with our obligation to preserve evidence for litigation.

ICT Systems Data (Internet history, email and messaging content, document access, saved documents)	Management Team IT Department	Pursuing the legitimate interests of the Data Controller, for the prevention and detection of crime, ensure compliance with rules, to pursue disciplinary action, to ensure contractual obligations to clients are being met.	The duration of employment and twelve years after the end of your employment, as set out by our regulator.
Mobile Phone Data (location data, usage, internet history, email and messaging records, call logs, photo and video recordings, data storage.)	Management Team IT Department	Pursing the legitimate interests of the Data Controller, for ensuring compliance with company mobile phone policy and for billing analysis	Duration of employment plus twelve months. (Limitation period of employment tribunal claims.)
Email Records (Personal data or sensitive personal data in emails used for personal matters).	Management Team IT Department	Pursuing the legitimate interests of the Data Controller, for the prevention and detection of crime, ensure compliance with rules, to pursue disciplinary action.	For the duration of the relevant Company project and twelve years after the project is completed. (Regulatory requirement.)
Disciplinary and Grievance Documentation (written complaints, witness statements, evidence, investigation notes, outcome correspondence, sanctions.)	Management Team Human Resources	Performance of the contract with the Data Subject. To ensure that the data subject is discharging their duties properly. Pursuing the legitimate interests of the Data Controller, to ensure employment rules are followed and investigate suspected misconduct and gross misconduct.	The duration of the Data Subject's employment and twelve months after termination. (Limitation period of employment tribunal claims.)
Voluntary Disclosure of Criminal Records	Management Team Human Resources	With the Consent of the Data Subject.	The duration of the Data Subject's employment and twelve months after termination. (Limitation period of employment tribunal claims.)
Performance Management Process (performance management targets, performance data, witness statements, evidence, meeting notes, sanctions, correspondence)	Management Team Human Resources	Performance of the contract with the Data Subject. To ensure that the data subject is discharging their duties. Pursuing the legitimate interests of the Data Controller.	The duration of the Data Subject's employment and twelve months after termination. (Limitation period of employment tribunal claims.)

Whistleblowing Disclosures/Investigations	Management Team Human Resources	Pursuing the legitimate interests of the Data Controller.	The duration of the Data Subject's employment and twelve months after termination. (Limitation period of employment tribunal claims.)
Social Media (Posts, usage, content.)	Management Team Human Resources IT Manager	Pursuing the legitimate interests of the Data Controller, to carry out recruitment checks, investigate disciplinary and grievance matters, ensure staff compliance with the Equality Act 2010. Any sensitive personal data processed will have been made public by the Data Subject.	The duration of the Data Subject's employment and twelve months after termination. (Limitation period of employment tribunal claims.)
Evidence of Qualifications (Certificates, Professional Memberships including RIBA, Records of training, CIAT, CPD)	Management Team Human Resources Administration Third party clients/regulators	For the performance of a contract with a Data Subject. To ensure the Data Subject is suitably qualified for the role.	The duration of the Data Subject's employment and twelve months after termination. (Limitation period of employment tribunal claims.)
Training Records (Confirmation of receipt of Handbook/policies. CPD Training)	Management Team Human Resources Administration Third party clients/regulators	Performing a contract with the Data Subject. Pursuing the legitimate interests of the Data Controller, to have appropriately trained staff.	The duration of the Data Subject's employment, and twelve months after termination. (Limitation period of employment tribunal claims.) Unless longer, for a regulatory reason.
Exit Interviews	Management Team Human Resources	Performing a contract with the Data Subject.	The duration of the Data Subject's employment, and twelve months beyond. (Limitation period of employment tribunal claims.)

References for Future Employers	Management Team Human Resources	We will seek the consent of exiting staff to retain and disclose Personal Data for the purpose of giving references.	The duration of the Data Subject's employment and seven years after termination. (Limitation period of civil breach of contract claims.)
Redundancy Processes	Management Team Human Resources	Complying with a legal obligation under the Employment Right Act 1996. Pursuing the legitimate interests of the Data Controller, to undertake cost saving measures if necessary.	The duration of the Data Subject's employment and seven years after termination. (Limitation period of civil breach of contract claims.)
Apprentice Application Forms, Apprenticeship Agreements, performance management and reviews, portfolios, applications and documentation relating to the Apprentice levy	Management and Human Resources. Third party supervisors at the apprentice's College, and/or qualification assessors. Third Party Payroll	For the performance of an eventual employment contract. For compliance with a legal obligation, in making declarations of information for receipt of the Apprentice levy.	For unsuccessful job applicants, seven months after the recruitment process. For successful applicants, the duration of your employment and seven years after termination of your employment. (Limitation period for civil breach of contract claims.)

The retention periods set out in this chart may be extended if there is the prospect of litigation with a Data Subject, and the Company is obliged to preserve documents for disclosure in actual or anticipated legal proceedings.

The Company may also be required from time to time to disclose Personal Data and/or Sensitive Personal Data to our regulator, in accordance with our professional and legal obligations.

The Company may from time to time disclose Personal Data and/or Sensitive Personal Data to their legal advisors to seek advice on the actual or potential establishment, exercise or defence of legal claims from staff. Measures will be taken to ensure compliance with GDPR principles, including but not limited to preserving the security and confidentiality of any such data.