OCRA (LONDON) LIMITED

Data Protection Policy

OCRA (LONDON) LIMITED
3RD Floor
14 Hanover Street
London
W1S 1YH
United Kingdom
T : 0207 317 0600
F: 0207 317 0610
E privacy@ocra.co.uk
www.ocra.co.uk

Contents

1 Interpretation

1.1 The terms in the left hand column of the following table have the meaning in the corresponding right hand column:

Company	OCRA (LONDON) LIMITED
Company Personnel	all employees, workers, contractors, agency workers, consultants, directors, managers, members and others who deal with Personal Data in the context of the Company's business.
Consent	agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.
Data Controller	the organisation that determines when, why and how to process Personal Data. The Company is the Data Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for the Company's commercial purposes.
Data Processing Record	the full and accurate record maintained by the DPM on the Company's behalf of Personal Data Processing.
Data Protection Legislation	(i) unless and until the GDPR is no longer directly applicable in the UK, the General Data Protection Regulation (2016/679) (GDPR) and any national implementing laws, regulations and secondary legislation as amended or updated from time to time in the UK and then (ii) any successor legislation to the GDPR or the Data Protection Act 1998.
Data Protection Manager (DPM)	the person with responsibility for data protection compliance for the Company (or their delegate from time to time).
Data Subject	a living, identified or identifiable individual about whom the Company holds Personal Data.
Data Subject Request	A request by a Data Subject to enforce rights listed in Schedule 2 of this Policy.
EEA	the countries included in the European Economic Area from time to time.
Explicit Consent	consent which requires a very clear and specific statement (that is, not just action).

Personal Data	any information identifying a Data Subject or information relating to a Data Subject that the Company can identify (directly or indirectly) from that data alone or in combination with other identifiers which the Company possesses or can reasonably access. Personal Data includes Sensitive Personal Data. Personal Data can be factual (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 the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that the Company or its third-party service providers put in place to protect it. The accidental or unlawful destruction, loss, alteration, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.
Privacy Policies	this Data Protection Policy and the Company's Data Security Policy and Data Breach Policy.
Privacy Notices	separate notices setting out information that may be provided to Data Subjects when the Company collects information about them.
Process or Processing	any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.
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. The Company also considers the following types of Personal Data to be of equivalent sensitivity to Sensitive Personal Data and therefore, for the purposes of this Policy, covered by this definition: [and] any [other] Personal Data which if used in an unauthorised manner might result in significant economic or social disadvantage to the Data Subject such as damage to confidentiality, equality of opportunity, financial situation or standing or reputation.

2 About this Policy

2.1 This Data Protection Policy sets out how the Company handles the Personal Data of its customers, suppliers, employees, workers and other third parties and should be read in conjunction with Company's Privacy Policies.

2.2 This Data Protection Policy applies to all Company Personnel. All Company Personnel must read, understand and comply with this Data Protection Policy and the Company's Privacy Policies when Processing Personal Data on the Company's behalf and attend training provided on its requirements.

2.3 Any breach of this Data Protection Policy or any other Privacy Policy may result in disciplinary action.

2.4 This Data Protection Policy does not form part of any Contract between the Company and Company Personnel or the Company and any other third party (including clients, customers and agents)

3 Personal data protection principles

3.1 The Company will adhere to the principles relating to Processing of Personal Data set out in the Data Protection Legislation which require Personal Data to be:

3.1.1 processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);

3.1.1 collected only for specified, explicit and legitimate purposes (Purpose Limitation);

3.1.2 adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);

3.1.3 accurate and where necessary kept up to date (Accuracy);

3.1.4 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 (Data Retention);

3.1.5 Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Data Security);

3.1.6 not transferred to another country without appropriate safeguards being in place (Cross Border Transfer Limitation);

3.1.7 made available to Data Subjects. In addition, Data Subjects must be allowed to exercise certain rights in relation to their Personal Data (Data Subject Requests).

3.2 The Company is responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

4 Lawfulness, fairness, transparency

4.1 Personal Data must be Processed lawfully, fairly and in a transparent manner.

4.2 Company Personnel may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. Data Protection Legislation restricts the Company's Processing of Personal Data unless there is a lawful basis for such Processing.

4.3 Lawful bases for Processing include:

4.3.1 the Data Subject has given his or her Consent;

4.3.2 the Processing is necessary for the performance of a contract with the Data Subject;

4.3.3 the Processing is necessary to meet the Company's legal obligations;

4.3.4 the Processing is necessary to protect the Data Subject's vital interests;

4.3.5 the Processing is necessary to pursue the legitimate interests of the Company or third parties provided such interests are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. Where the Company Processes Personal Data based on a legitimate interests basis, the legitimate interests must be set out in appropriate Privacy Notices.

4.4 Where the Company proposes to Process Sensitive Personal Data, additional conditions must be satisfied which may include obtaining the Data Subject's Explicit Consent. You should consult with, and seek approval from, the DPM prior to Processing any Sensitive Personal Data.

4.5 The Company must identify and document in its Data Processing Record the legal basis being relied on for each Processing activity. It is your responsibility to notify to the DPM any processing for which you have responsibility. It is the responsibility of the DPM to record the Processing in the Company's Data Processing Record.

4.6 The Data Protection Legislation requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible and in clear and plain language so that a Data Subject can easily understand them.

5 Purpose limitation

5.1 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

5.2 You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes (and they have Consented, where necessary).

6 Data minimisation

6.1 Personal Data must be adequate, relevant and limited to what is necessary for the purposes for which it is Processed.

6.2 You may only collect Personal Data that you require for your job duties and should not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

6.3 You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

6.4 You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's Data Retention Policy (See Schedule 1).

7 Accuracy

7.1 Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

7.2 You will take all reasonable steps to ensure that the Personal Data the Company uses and holds is accurate, complete, kept up to date and relevant to the purpose for which it was collected.

7.3 You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards in accordance with the Company's Data Retention Policy (See Schedule 1). You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

8 Data Retention

8.1 You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which it was originally collected, including for the purpose of satisfying any legal, accounting or reporting requirements.

8.2 You must comply with the Company's Data Retention Policy (See Schedule 1) which recommends the periods after which Personal Data should normally be anonymised, deleted or destroyed.

8.3 You will take all reasonable steps to destroy or erase from the Company's systems all Personal Data that the Company no longer requires in accordance with all the Company's Data Retention Policy (See Schedule 1). You should seek the assistance of the Company's IT Department as is appropriate. You should also consider requiring third parties to delete Personal Data where appropriate.

8.4 You will ensure Data Subjects are informed of the period for which data is stored in any applicable Privacy Notice.

9 Data Security

9.1 Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing and against accidental loss, destruction or damage.

9.2 The Company will develop, implement and maintain safeguards appropriate to its size, scope and business, available resources, the amount of Personal Data that is owned or maintained on behalf of others and identified risks. The Company will regularly evaluate and test the effectiveness of those safeguards to ensure security of its Processing of Personal Data.

9.3 You are also responsible for protecting the Personal Data the Company holds. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data in accordance with the Company's Data Security Policy and other instructions, guidance or technological applications issued by the Company from time to time. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

9.4 You may only transfer Personal Data to third-party service providers who agree to comply with such policies and procedures as the Company requires and which agree to put adequate measures in place.

9.5 You must not attempt to circumvent the administrative, physical and technical safeguards the Company maintains to protect Personal Data. Failure to comply with the Company's Data Security Policy will be dealt with in accordance with the Company's Disciplinary Policy and may result in dismissal.

10 Cross Border Transfer limitation

10.1 The Data Protection Legislation restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to Data Subjects by the Data Protection

Legislation is not undermined. Personal Data is transferred across borders when it is transmitted or sent from the country in which it originates to a different country or when it is viewed or accessed from a different country.

10.2 You may only transfer Personal Data outside the EEA if [you have the written authority of the DPM.

11 Data Subject's Requests

11.1 A Data Subject Request is a request made by or on behalf of a Data Subject to enforce their rights pursuant to Data Protection Legislation. Potential Data Subject Requests and how the Company should respond to them are set out in Schedule 2 to this Policy.

11.2 Only Company Personnel authorised by the DPM shall respond to Data Subject Requests.

11.3 It is important to be satisfied of the Data Subject's identity prior to complying with any Data Subject Request. If there is any doubt you should ask for further evidence to verify their identity; for example we may request confirmation of online signature information provided to us at initial stages of contract.

11.4 If a Data Subject Request is made on behalf of a Data Subject, you must ensure that the person making the request is entitled to act on behalf of the Data Subject. You must request a copy of a written authority to make the request.

11.5 Data Subject Requests must receive a prompt response and, in any event, no later than **one month** of the date on which the request is received. This can be extended in limited circumstances as advised by the DPM.

11.6 The Company shall not charge a fee when responding to a Data Subject Request, unless the request is manifestly unfounded or excessive. In such instances the Company may charge a reasonable fee that takes into account the administrative costs of taking the necessary action to respond. You should consult with the DPM for guidance on this issue before discussing any fee with the Data Subject.

11.7 Where the request is unfounded or unreasonable it is possible to refuse to act on the request. You should always seek guidance from the DPM before rejecting a Data Subject Request on these grounds.

11.8 In limited circumstances, the Company may be exempt from complying (in whole or in part) with the Data Subject Request. Exemptions may apply, for example, for reasons relating to the public interest, the prevention of crime or for reasons relating to legal proceedings. You should take advice from the DPM if you consider that an exemption may apply in relation to a Data Subject Request.

11.9 The Company is required to respond to a Data Subject Request in relation to Personal Data held at the time the request was received. Under no circumstances should Company Personnel amend or delete Personal Data other than in the ordinary course of business.

12 Role of the DPM

12.1 Company Personnel must always contact the DPM for advice and guidance in the following circumstances:

12.1.1 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) see section 4.3.

12.1.2 if you need to rely on Consent and/or need to capture Explicit Consent (see section 4.3);

12.1.3 if you need to draft Privacy Notices (see section 4.6);

12.1.4 if you are unsure about the retention period for the Personal Data being Processed (see section 8);

12.1.5 if you are unsure about what security or other measures you need to implement to protect Personal Data (see section 9);

12.1.6 if there has been a Personal Data Breach (see section 13);

12.1.7 if you are unsure on what basis to transfer Personal Data outside the EEA (see section 10);

12.1.8 if you need any assistance dealing with a Data Subject Request (see section 11) and, in particular, if you intend to rely on an exemption or are intending not to comply (in whole or in part with the request) or charge a fee;

12.1.9 whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see section 14) or plan to use Personal Data for purposes incompatible with those it was collected for;

12.1.10 if you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making [(see section 14)];

12.1.11 if you intend to carry out direct marketing activities [(see section 15)]; or

12.1.12 if you intend to share Personal Data with third parties (see section 16).

13 Reporting a Personal Data Breach

13.1 The Data Protection Legislation requires Data Controllers to notify certain Personal Data Breaches to the Information Commissioner's Office (**ICO**) and, in some instances, the Data Subject.

13.2 The Company has a Data Breach Policy to deal with any suspected Personal Data Breaches and will notify the ICO or Data Subjects where it is legally required to do so.

13.3 If you know or suspect that a Personal Data Breach has occurred, do not attempt to respond to the incident yourself. Immediately contact the DPM and follow the Data Breach Policy. You should preserve all evidence relating to the potential Personal Data Breach.

14 Accountability

Record keeping

14.1 The Company to keeps full and accurate records of all its data Processing activities (Data Processing Record).

14.2 You must assist the Company in keeping and maintaining an accurate Data Processing Record reflecting its Processing (including records of Data Subjects' Consents, where applicable).

14.3 The Data Processing Record should include, as a minimum, the name and contact details of the Data Controller and the DPM, clear descriptions of the types of Personal Data, categories of Data Subjects, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, Personal Data retention periods and a description of the security measures in place.

Training and audit

14.4 You must undergo all mandatory data privacy related training and ensure that any Company Personnel reporting to you undergo similar mandatory training.

14.5 You must regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

Privacy By Design and Data Protection Impact Assessment

14.6 The Company is required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures in an effective manner, to ensure compliance with data privacy principles.

14.7 When contemplating the implementation of any programs, systems, or processes that Process Personal Data you must consult with the DPM about what Privacy by Design measures may be appropriate.

Automated Decision-Making

14.8 Automated Decision-Making is generally prohibited when a decision has a legal or similar significant effect on an individual. If a decision is to be based solely on Automated Processing, then you must consult with and follow any guidance issued by the DPM.

15 Direct marketing

15.1 The Company is subject to certain rules and privacy laws when marketing to its customers. You must consult with and follow any guidance issued by the DPM in connection with any initiative in relation to direct marketing. A Data Subject's objection to direct marketing must be promptly honoured.

16 Sharing Personal Data

16.1 Generally, the Company is not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

16.2 You may only share the Personal Data the Company holds with another employee, agent or representative of the Company if the recipient has a job-related need to know the information [and the transfer complies with any applicable cross-border transfer restrictions.]

16.3 You may only share the Personal Data the Company holds with third parties, such as our service providers, if:

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

16.3.2 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;

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

16.3.4 the transfer complies with any applicable cross border transfer restrictions; and

16.3.5 a fully executed written contract that contains approved third party clauses has been obtained.

17 Changes to this Data Protection Policy

17.1 The Company reserves the right to change this Data Protection Policy at any time without notice. It is your responsibility to ensure that your knowledge of this Data Protection Policy is up to date and that you comply with its terms.

17.2 This Data Protection Policy does not override any applicable national data privacy laws and regulations in countries where the Company operates.

18 Acknowledgement of receipt and review

18.1 I, acknowledge that I received and read a copy of OCRA (LONDON) LIMITED's Data Protection Policy and Privacy Policies referred to on the date given below and understand that I am responsible for knowing and abiding by their terms.

Signed …….

Printed Name …….

Date …….

Schedule 1 Data Retention Periods

Data Subject	Personal Data	Accuracy Check	Retention Period
Unsuccessful Job Candidates	CVs Disability Data	n/a	[6/12] months post campaign
Successful Job Candidates	CVs Disability Data	n/a	7 years after employment 7 years after employment
Employees	Employee Record Contact Details General data Right to work Data Health data Injury Records Maternity Pay Data	 Annually Annually	 7 years after employment 7 years after employment 3 years after employment [4 years or 40 years] 4 years 4 years from end of tax year
Employees	Payroll Record Bank Details Tax Details/PAYE Records Pension Contribution Details		7 years after employment On termination of employment 7 years after employment 7 years
Contractors	Supplier Record Contact Details	 Annually	 7 years
Contractors	Payment Records Bank Details Tax Details (if any)		 On termination of engagement 7 years
Existing Customers	Contact Details	Annually	6 years in line with MLR 2017/HMRC Trust & Corporate Service Providers Guidance and OCRA (LONDON) LIMITED Compliance

			Manual
Existing Customers	Purchase History	Annually	6 years in line with MLR 2017/HMRC Trust & Corporate Service Providers Guidance and OCRA (LONDON) LIMITED Compliance Manual
Potential Customers	Contact Details	Annually	12 months post campaign
Suppliers	Contact Details Purchase History	Annually	End of supplier relationship

Note: the data subjects, types and retention periods are suggested only. The Schedule should be tailored to your business and specific requirements having in mind the requirement not to keep personal data longer than is necessary for the purpose for which it was collected.

Schedule 2 Data Subject Rights and Requests

Description of Right or Request	How to Respond
Right to Information Data Subjects have the right to receive information about how the Company collects Personal Data and the Company's Processing activities. Data Subjects have the right to be informed if their Personal Data is to be used for a purpose different to the purpose for which it was collected. Data Subjects have the right to be notified of any breach in relation to their Personal Data.	The Company must provide information to the Data Subject at the time Personal Data is collected in an appropriate Privacy Notice If information is collected from a third party, a Privacy Notice must be provided to the Data Subject within a reasonable period of time, and at the latest within one month. Information should be provided in writing using a clear and plain language and in a concise, transparent and intelligible manner and should be easily accessible. It is not necessary for the Company to provide the information where the Data Subject already has the information. Notification to a Data Subject of a Data Breach may only be made by the DPM in accordance with the Company's Data Breach Policy.

Right of Access
 	
A Data Subject is entitled to:
 	
• know that the Company is Processing their Personal Data;
• access their Processed Personal Data in an intelligible and accessible format, unless this adversely affects the rights and freedoms of others;
• receive information about the Processing (similar to that included in a Privacy Notice);
• be notified of their rights to:
  ○ request correction or erasure of Personal Data;
  ○ restrict or object to certain types of Processing; and
  ○ make a complaint to the ICO.
	Subject to section 11 of this Policy, Company Personnel shall:
	
	• search databases, systems, applications and other places where the Personal Data may be held; and
	• confirm to the Data Subject whether or not their Personal Data is being Processed by the Company;
	• provide the required information to the Data Subject.
	
	Particular care must be taken not to prejudice the privacy of other Data Subjects in complying with the Data Subject's request.
	
	The Company may refuse to respond to such requests or charge a fee in relation to such requests where requests are unfounded or excessive or where a relevant exemption applies.

Data Portability Data Subjects are entitled to receive a copy of certain Personal Data in a commonly used and machine-readable format so that they are able to store it for further use on a private device Data Subjects can also request their Personal Data be	Subject to section 11 of this Policy, Company Personnel shall: • search databases, systems, applications and other places where the Personal Data may be held;

transmitted to another Data Controller. This right only applies in relation to Personal Data provided to the Company by the Data Subject which is processed by automated means based on the Data Subject's Consent or for the purpose of a contract.	• provide a copy of the Personal Data to the Data Subject; • or, if the Data Subject has requested it, transmit the Personal Data directly to another party, where technically feasible. Particular care must be taken not to prejudice the privacy of other Data Subjects in complying with the Data Subject's request.
Correction A Data Subject is entitled to request that the Company corrects inaccurate and/or completes incomplete Personal Data. A correction request may be made orally or in writing.	Subject to section 11 of this Policy, Company Personnel shall: • make a written record of any oral requests; • where practicable, restrict further Processing of the relevant Personal Data; • determine whether or not a correction is appropriate; and • where a correction is appropriate: ○ correct the Personal Data without undue delay; ○ inform any third party to whom the Personal Data has been disclosed of the correction request (unless it is impossible or involves disproportionate effort); ○ inform the Data Subject about such recipients if the Data Subject so requests; or • where a correction is not appropriate: ○ inform the Data Subject of the decision and the reasons for it; ○ advise the Data Subject of their rights to complain to the ICO; ○ keep a record of the Data Subject's reasons for suggested inaccuracy.
Erasure ("right to be forgotten") A Data Subject has the right to request erasure of their Personal Data where (and only where): • the Personal Data is no longer necessary for the purpose that the Company collected it; • the Data Subject withdrew Consent to the Company's Processing activities (and no other legal justification for Processing applies); • the legal basis for Processing is legitimate interests, the Data Subject has objected to Processing and the legitimate interests basis cannot be substantiated; • the Data Subject objects to Processing for direct marketing purposes; • the Company unlawfully Processed the Personal Data; • the Company has a legal obligation to erase the Personal Data; or • the Company collected the Personal Data in the context of offering online services to children.	Subject to section 11 of this Policy, Company Personnel shall: • make a written record of any oral requests; • search databases, systems, applications and other places to identify relevant Personal Data; • consider whether the Personal Data may be retained on grounds that it is required for a legitimate reason (see below); • where there is no legitimate reason to retain the Personal Data: ○ erase the Personal Data without undue delay; ○ where the Personal Data has been made public, take reasonable steps to inform those who are Processing the Personal Data that the Data Subject has requested the erasure of any links to, or copies of, their Personal Data; ○ inform any third party to whom the Personal Data has been disclosed of the erasure request, unless it is impossible or involves disproportionate effort.

A request for erasure may be made orally or in writing.	○ inform the Data Subject about such recipients if the Data Subject so requests. Legitimate reasons for retaining Personal Data despite an erasure request will include, for example, to comply with a legal obligation or to establish, exercise or defend legal claims. Where a decision is made not to erase the Personal Data, Company Personnel must: o inform the Data Subject of the decision and the reasons for it; o advise the Data Subject of their rights to complain to the ICO; Company Personnel should seek advice from the DPM before erasing data, relying on any exemption or legitimate reason not to erase Personal Data.
Restriction Data Subjects are entitled to restrict Processing of their Personal Data by the Company when one of the following applies: • the Data Subject contests the accuracy of the Personal Data - Processing must be restricted until its accuracy is verified; • the Data Subject objects to Processing where the lawful basis for Processing is legitimate interests – Processing must be restricted until it can be verified whose competing interests should prevail; • the Processing is unlawful - the Data Subject can request that the Company restricts Processing as an alternative to erasure; • the Company no longer needs to Process the Personal Data, but the Data Subject needs it for the establishment, exercise, or defence of legal claims. A restriction request may be made orally or in writing.	Subject to Section 11 of this Policy, Company Personnel shall: • make a written record of any oral requests • restrict further Processing of the Personal Data whilst the grounds for the request (accuracy, lawfulness, legitimate interests) are investigated; • inform any recipient of the Personal Data about the restriction request, unless it is impossible or involves disproportionate effort; • inform the Data Subject about such recipients if they so request; • only lift any restriction, once the Data Subject has been informed of the lifting of the restriction, the reasons for it and the Data Subject's right to make a complaint to the ICO. The Company may continue to Process the Personal Data: • with the Data Subject's consent; • in the exercise of defence of legal claims; • to protect the rights of other person(s); or • for important public interest reasons.
Right to Object Data Subjects are entitled to object to Processing of their Personal Data where Processing is being carried out: • on the legal basis that it is necessary for the Company's or a third party's legitimate interests. • for direct marketing purposes, including profiling	Subject to section 11 of this Policy, Company Personnel must: • restrict processing whilst the Data Subject's request is considered; • cease Processing the Personal Data, unless the

related to direct marketing; • for scientific or historical research purposes or statistical purposes (unless the processing is necessary in the public interest).	Company can demonstrate: ○ a compelling legitimate ground that overrides the Data Subject's interests and reasons for objection; or ○ continued Processing is necessary to establish, exercise, or defend legal claims. Where the Company decides that further Processing is appropriate the Data Subject must be informed of the decision before further Processing is undertaken, the reason for the decision and the Data Subject's rights to complain to the ICO. Where an objection is raised to Processing for direct marketing purposes, Processing must cease immediately without exception.