Privacy Policy

Oxford Employment law solicitors for clients and potential clients overview.

Oxford Employment Law Solicitors ("OELS" or "we") take the security and privacy of your data seriously. We need to gather and use information or 'data' about clients and potential clients, as part of our business and to manage our relationship with clients and potential clients. In this privacy policy clients and potential clients will be referred to as "you".

We intend to comply with our legal obligations under the Data Protection Act 2018 (the "2018 Act") and the EU General Data Protection Regulation ("GDPR") in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

This policy applies to current and former clients, as well as potential clients providing personal data to us through on-line enquiries, telephone conversations, meetings or otherwise. If you fall into one of these categories then you are a 'data subject' for the purposes of this policy. You should read this policy alongside our terms of engagement and any other notice we issue to you from time to time in relation to your data.

We have measures in place to protect the security of your data, such as password protection, access limited solely to authorised persons, and passcode protected storage facilities.

We shall retain your personal data in accordance with the data protection principles and the GDPR (see section 9 below). We will only hold data for as long as necessary for the purposes for which we collected it.

OELS is a 'data controller' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.

This policy explains how we will hold and process your information. It explains your rights as a data subject.

This policy does not form part of our terms of engagement with you and can be amended by OELS at any time. It is intended that this policy is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this policy, we intend to comply with the 2018 Act and the GDPR.

Data Protection Principles

Personal data must be processed in accordance with six 'Data Protection Principles.' It must:

be processed fairly, lawfully and transparently;
be collected and processed only for specified, explicit and legitimate purposes;
be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
not be kept for longer than is necessary for the purposes for which it is processed; and
be processed securely.
We are accountable for these principles and must be able to show that we are compliant.

How we define personal data

‘Personal data’ means information which relates to a living person who can be identified from that data (a ‘data subject’) on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

This policy applies to all personal data whether it is stored electronically, on paper or on other materials.
This personal data might be provided to us by you, or someone else (such as your employer or former employer, or your doctor), or it could be created by us.
We may collect and use the following types of personal data about you:
your contact details and date of birth;
your gender;
your marital status and family details;
information about your employment and employment history including start and end dates of employment, role and location, working hours, details of promotion, salary, pension, benefits and holiday entitlement;
your bank details and information in relation to your tax status including your national insurance number;
your identification documents including passport and driving licence and information in relation to your immigration status and right to work;
information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings);
information relating to your performance and behaviour at work;
training records;
any other category of personal data which we may notify you of from time to time.
How we define special categories of personal data
‘Special categories of personal data’ are types of personal data consisting of information as to:
your racial or ethnic origin;
your political opinions;
your religious or philosophical beliefs;
your trade union membership;
your genetic or biometric data;
your health;
your sex life and sexual orientation; and
any criminal convictions and offences.
We may hold and use any of these special categories of your personal data in accordance with the law.

How we define Processing

‘Processing’ means any operation which is performed on personal data such as:
collection, recording, organisation, structuring or storage;
adaption or alteration;
retrieval, consultation or use;
disclosure by transmission, dissemination or otherwise making available;

alignment or combination; and
restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

How will we process your personal data?
We will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.
We will use your personal data for:
performing legal services for you as our client;
complying with any legal obligation; or
if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights in section 12 below.

We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

If you choose not to provide us with certain personal data you should be aware that we may not be able to perform out certain parts of the contract between us.

Examples of when we might process your personal data

We have to process your personal data in various situations during our engagement with you and even following termination of our engagement.
For example (and see section 7.6 below for the meaning of the asterisks):
to decide whether to engage with you;
to decide terms of engagement;
to carry out legal services for you as our client*;
to monitor and protect the security (including network security) of OELS, of you, our other staff, agents, other clients and others;
monitoring compliance by you, us and others with our policies and our contractual obligations*;
to comply with the Solicitors Regulation Authority and Law Society rules, regulations, policies and procedures, and any other laws and regulations which affect us or apply to us*;
to answer questions from insurers in respect of any insurance policies which relate to you*;
running our business and planning for the future;
the prevention and detection of fraud or other criminal offences;
to defend OELS in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure*; and
for any other reason which we may notify you of from time to time.
We will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting Justin Godbolt, partner.
We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

where it is necessary for carrying out rights and obligations required by law;
where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
where you have made the data public;
where processing is necessary for the establishment, exercise or defence of legal claims; and
where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.
We might process special categories of your personal data for the purposes in paragraph 7.2 above which have an asterisk beside them. In particular, we will use information in relation to:
your race, ethnic origin, religion, sexual orientation or gender to monitor equality; and
your sickness absence, health and medical records, fitness for work, to comply with our legal obligations and in order to provide legal services to you where such information is relevant to your case.
We do not take automated decisions about you using your personal data or use profiling in relation to you.

Retention of your personal data

We will retain your information only for as long as is necessary for the purposes for which we collected it as set out in this Privacy Policy. If you no longer wish for us to retain information we hold about you, you may require that we delete such information, unless we need to retain and use your information to comply with our legal obligations, to resolve disputes, to enforce our agreements, in order to perform a contract we have with you (such as a current client), or otherwise permitted or required by law.

Sharing your personal data
We shall not share your personal data without your express consent.

How to deal with data breaches

We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals then we must also notify the Information Commissioner's Office within 72 hours.
Subject access requests
Data subjects can make a 'subject access request' ('SAR') to find out the information we hold about them. This request must be made in writing to Justin Godbolt, partner.
We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.
There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.
Your data subject rights
You have the right to information about what personal data we process, how and on what basis as set out in this policy.
You have the right to access your own personal data by way of a subject access request (see above).
You can correct any inaccuracies in your personal data. To do you should contact Justin Godbolt, partner.

You have the right to request that we erase your personal data where we were not entitled or required under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you should contact Justin Godbolt, partner.
While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact Justin Godbolt, partner.
You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.
You have the right to object if we process your personal data for the purposes of direct marketing.
You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.
With some exceptions, you have the right not to be subjected to automated decision-making.
You have the right to be notified of a data security breach concerning your personal data.
In most situations we will not rely on your express consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact Justin Godbolt, partner.
You have the right to complain to the Information Commissioner. You can do this be contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (ico.org.uk). This website has further information on your rights and our obligations.