



Our Ref: POL-IT-001
Date: 11 March 2025

HURLEY & DAVIES

DATA PROTECTION AND PRIVACY POLICY

Hurley and Davies Ltd, here-after referred to as '**the Company**', need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We take the security of your data seriously and are committed to protecting your privacy and processing your personal data in accordance with the Data Protection Legislation defined under the General Data Protection Regulations (GDPR).

This policy covers how we securely collect, use, store, process and disclose the data that you supply to us and your rights about data that we hold about you.

It also explains your obligations when obtaining, handling, processing, or storing personal data in the course of working for, or on behalf of the Company.

It applies to current and former employees, workers, volunteers, interns, apprentices, and consultants. 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 your contract of employment (or contract for services, if relevant) and any other notice we issue to you from time to time in relation to your data.

The Company has taken steps to protect the security of your data in accordance with this policy and will train staff about their data protection responsibilities as part of the induction process. We will only hold data for as long as necessary and solely for the purposes for which we collected it.

The Company 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 does not form part of your contract of employment (or contract for services, if relevant) and can be amended by the Company at any time.

Data Protection Officer

Hannah Morgan is the Company's Data Protection Officer and is responsible for reviewing this policy on the Company's data protection responsibilities and any risks in relation to the processing of data. You should direct any queries and concerns regarding the processing of your personal data, or the contents of this policy to her.

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 (i.e., the '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 where the individual's identity has been removed. This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

The Personal Data We Collect About You

The types of personal data that we collect and use about you are categorised below:

Code	Description
PC	Personal contact details such as name, title, addresses, telephone numbers, and email addresses.
DOB	Date of birth.
G	Gender.
MSD	Marital status.
NOK	Next of kin and emergency contact information.
NI	National Insurance Number.
FI	Bank account details, payroll records, travel logs and expenses and tax status information.
EB	Salary, annual leave, pension, and benefits information.
SD	Start and end dates.
WL	Location of employment or workplace.
DVLA	Motor Vehicle Insurance information.
RI	Recruitment information (including copies of right to work documentation, passport, references, and other information included in a CV or cover letter or as part of the application process).
ER	Employment records (including job titles, work history, working hours, training records and professional memberships).
PER	Performance information.
DG	Disciplinary and grievance information.
ICS	Information about your use of our information and communications systems.
P	Photographs.

We may also collect, store and use **‘special categories’** of more sensitive personal data which require a higher level of protection.

How We Define ‘Special Categories’ of Personal Data

‘Special categories’ of personal data relate to information about:

- 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.

The types of special categories of your personal data that we may collect and use about you are categorised below:

Code	Description
HR	Information about your health, including any medical condition, health, and sickness records (including Occupational Health records).
A	Absence notes
ED	Information about your race or ethnicity, religious beliefs, sexual orientation, and political opinions.
TU	Trade union membership.
GI	Genetic information and biometric data.

How Personal Data is Collected

Personal data might be provided to us by you, or someone else (such as an employment agency, a former employer, your doctor, or a credit reference agency), or it could be created by us. It could be provided or created during the application and recruitment process or during the course of the contract of employment (or services) or after its termination. It could be created by your manager or other colleagues in the course of undertaking job-related activities throughout your period of employment with us.

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 We Process Your Personal Data

The Company will process your personal data, including special categories of personal data, for:

- performing the contract of employment (or services) between us [**CONTRACTUAL**];
- complying with any legal obligation [**LEGAL**]; or
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else) [**INTEREST**]. 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.

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.

Non-exhaustive examples regarding how we might process your personal data and our lawful basis for doing so are detailed below:

Purpose	Data Categories	Lawful Basis
Making a decision about your recruitment or appointment.	PC, RI, ER	[INTEREST]
Determining the terms on which you work for us.	EB, SD, PC, RI, ER	[INTEREST]
Checking you are legally entitled to work in the UK.	PC, DOB, NI, DVLA	[LEGAL]
Paying you and, if you are an employee, deducting tax and National Insurance contributions.	PC, NI, FI, SD	[INTEREST]
If benefits apply to you	PC, DOB, G, MSD, NOK, NI, FI, EB, SD	[CONTRACTUAL]
Liaising with your pension provider.	PC, DOB, NI, EB, SD	[CONTRACTUAL]
Administering the contract we have entered into with you.	PC, NOK, NI, FI, EB, SD, WL, PER, DG	[INTEREST] [CONTRACTUAL]
Business management and planning, including accounting and auditing.	PC, DOB, G, NI, FI, EB, SD, WL, PER, DG, ICS, HR, ED, TU	[INTEREST]
Conducting performance reviews, managing performance, and determining performance requirements.	PC, EB, SD, WL, PER, DG, ICS, ED	[INTEREST] [CONTRACTUAL]
Making decisions about salary reviews and compensation.	PC, FI, EB, SD, WL, RI, ER, PER, DG, ICS	[INTEREST] [CONTRACTUAL]
Assessing qualifications for a particular job or task, including decisions about promotions.	PC, RI, ER, PER, DG, ED	[INTEREST] [CONTRACTUAL]
Gathering evidence for possible grievance or disciplinary hearings. Making decisions about your continued employment or engagement.	PC, PER, DG, ICS, ED PC, PER, DG, ICS, ED	[INTEREST] [CONTRACTUAL]
Making arrangements for the termination of our working relationship.	PC, NI, FI, EB, PER, DG, ED	[INTEREST] [CONTRACTUAL]
Education, training, and development requirements.	PC, ER, PER, DG, ED	[INTEREST] [CONTRACTUAL]
Dealing with legal disputes involving you, or other employees, workers, and contractors, including accidents at work.	PC, FI, EB, COM, PER, DG, ICS, P, HR, A, ED, GI	[INTEREST]
Ascertaining your fitness to work and managing sickness absence.	PC, DOB, G, MSD, NOK, WL, PER, DG, ICS, P, HR, ED	[INTEREST] [CONTRACTUAL]
Complying with health and safety obligations.	PC, NOK, WL, ED	[LEGAL] [CONTRACTUAL]
To prevent fraud.	PC, NI, FI, DVLA, RI, ER, GI	[INTEREST]
To monitor your use of our information and communication systems to ensure compliance with our IT policies.	PC, ICS	[INTEREST]
To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.	PC, ICS	[INTEREST]
To conduct data analytics studies to review and better understand employee retention and attrition rates.	PC, DOB, G, MSD, HR, ED	[INTEREST]
Equal opportunities monitoring.	PC, DOB, G, MSD, HR, ED	[INTEREST]

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 employee benefits), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

How We Process Your ‘Special Categories’ of Personal Data

‘Special categories’ of particularly sensitive personal data as defined above require higher levels of protection and we will only process such data 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 the Company’s Data Protection Officer.

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 under employment 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 stated above, and in particular, we may use information in relation to:

- your race, ethnic origin, religion, sexual orientation, or gender to monitor equal opportunities;
- your leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws;
- 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 and to administer benefits; and
- your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members.

We do not take automated decisions about you using your personal data or use profiling in relation to you.

Data About Criminal Convictions

We may only use data relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with this policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary 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 employees or former employees in the course of legitimate business activities with the appropriate safeguards.

We envisage that we will hold information about criminal convictions and access your DBS portal.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. 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.

Your Duty to Inform Us of Changes

It is important that the personal data we hold about you is accurate and current, so please let us know if your data changes.

Disclosure/Data Sharing

We may have to share your data with third parties, including third-party service providers (including contractors and designated agents); other entities in the group; in the context of a sale of the business; or with a regulator or to otherwise comply with the law; our insurers and/or professional advisers to manage risks legal disputes.

The following activities are carried out by third-party service providers:

- Payroll, pension administration, and benefits provision and administration.
- Statutory accounts preparation.
- IT services.

We share your data with these 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. We require those service providers to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

We do not send your personal data outside the European Economic Area. If this changes, you will be notified of this and the protections which are in place to protect the security of your data will be explained.

Data Retention

We must store most of your HR data for a period of at least 6 years following the termination of your employment, some personal financial data will be destroyed after 2 years, and Health and Safety information must be held for a minimum of 40 years.

Your 'Data Subject' Rights

- You have the right to know 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 below).
- You can correct any inaccuracies in your personal data by contacting the Company's Data Protection Officer.
- You have the right to request that we erase your personal data where we were not entitled 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 the Company's Data Protection Officer.
- 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 the Company's Data Protection Officer.
- 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 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 the Company's Data Protection Officer.

How You Should Process Personal Data for the Company

Everyone who works for, or on behalf of, the Company has some responsibility for ensuring data is collected, stored, and handled appropriately, in line with this policy and the Company's IT policies.

You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of the Company and only if you are authorised to do so for the specified lawful purpose for which it was obtained:

- You should not share personal data informally.
- You should keep personal data secure and not share it with unauthorised people.
- You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.
- You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.
- You should use strong passwords.
- You should lock your computer screens when not at your desk.
- Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.
- Do not save personal data to your own personal computers or other devices.
- Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the Company's Data Protection Officer.
- You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.
- You should not take personal data away from Company's premises without authorisation from your line manager or the Company's Data Protection Officer.
- Personal data should be shredded and disposed of securely when you have finished with it.
- You should ask for help from the Company's Data Protection Officer if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.
- Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.
- It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

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.

If you are aware of a data breach you must contact the Company's Data Protection Officer immediately and keep any evidence you have in relation to the breach.

Subject Access Request

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. If you receive such a request, you should forward it immediately to the Company's Data Protection Officer who will coordinate a response.

If you would like to make a SAR in relation to your own personal data, you should make this in writing to the Company's Data Protection Officer. 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.

Complaints & Questions

If you have any questions about this policy or how we handle your personal information, please contact the Company's Data Protection Officer. If we have breached our duty of care, we will take appropriate action.

If you are not satisfied by our response, you also have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues:

Web: www.ico.org.uk

Email: casework@ico.org.uk

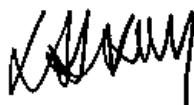
Changes To This Policy

We reserve the right to update this policy 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 data.

Directors' Approval



Andrew Davies



Luke Hurley



Chris Davies



Stuart Roberts