Employee Privacy Notice

What is the purpose of this document?

The intention of this Privacy Notice is to inform you of the Personal Data that is processed for the purpose of the business and for your benefit. This privacy notice will cover various stages of your employment with the Data Controller, including your recruitment stages, and the personal data that may be requested if you decide to leave the Company's employment.

Who is the Data Controller?

The Data Controller of your personal data is your employing company. This means it will be:

Webevents Limited T/A WMG, Ingenuity Digital and Equation incorporated and registered in England and Wales with company number 3984604 whose registered office is at 1st Floor Central House, Beckwith Knowle, Otley Road, Harrogate, HG3 1UF; or

IDHL Web Limited T/A NetConstruct, Pinpoint, Statement, Fostr and Ampersand incorporated and registered in England and Wales with company number 14218662 whose registered office is at 1st Floor Central House, Beckwith Knowle, Otley Road, Harrogate, HG3 1UF; or

IDHL Technology Limited T/A Wired Plus and Snow.IO incorporated and registered in England and Wales with company number 14225124 whose registered office is at 1st Floor Central House, Beckwith Knowle, Otley Road, Harrogate, HG3 1UF.

What is the Data Controller processing my Personal Data for?

We need all the categories of information in the list below primarily to allow us to perform our contract with you and to enable us to comply with legal obligations.

In some cases we may use your personal data to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests.

We have indicated the purpose or purposes for which we are likely to process or will process your personal data. These include:

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Paying you and deducting tax and National Insurance contributions.
- Providing benefits to you (these will be provided to you following two years service).
- Liaising with your pension provider.
- Administering the contract we have entered into with you.
- Business management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular role or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Processing your leaving feedback and information.
- Processing and providing for references post-employment.
- Education, training and development requirements.

- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- Preventing fraud.
- Monitoring your use of our information and communication systems to ensure compliance with our IT policies.
- Ensuring network and information' security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- Conducting data analytics studies to review and better understand employee retention rates.
- Equal opportunities monitoring.
- Providing internal IT support.

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

What Personal Data may the Data Controller hold on you?

During your employment with the Data Controller, the personal data listed below may be collected for a range of legitimate interests which are explained in the section above:

- Address
- Bank Details
- Benefits Deductions
- Benefits Membership numbers
- Bonuses and commissions
- Car allowance
- Car Registration number
- CCTV footage
- Childcare Contributions
- Company Car details
- Criminal Convictions
- Disabilities
- DOB
- Email Address
- Employment History
- Ethnic Origin
- Exit interview notes
- Family personal data – including but not limited to name, DOB and address
- Full name
- Gender
- Personal Grievance/ Disciplinary information
- Photographs
- Probation period
- Passport/Birth certificate copy
- Paycare contributions
- Payroll numbers
- Penalties of disciplinaries
- Pension deductions and contributions
- Performance reviews
- Qualifications
- Test results
- Witness statements
- Work permit information
- General personal data regarding history, hobbies and interests
- GP Information/Details
- Hardware properties (inclusive of company provided and personally owned devices if used on our networks)
- Holidays
- Hours of work
- ID Badge unique number
- Interview notes
- Job title
- Leaving date
- Line manager
- Marital status
- Medical details
- Member premiums
- Next of kin/ contact number
- NI number
- Outcomes of grievances
- P45/46 details
- Parking space
- References
- Religion or belief
- Reporting manager
- Sick/holiday calculations
- Start date
- Salary details
- Sexual orientation
- Telephone numbers

The following pieces of Personal Data are considered to be "Sensitive Personal Data":

- Ethnic Origin
- Sexual orientation
- Religion or belief
- Physical health conditions
- Mental Health conditions

How will we use your Personal Data?

We will only use your personal data when the law allows us to.

Most commonly, we will use your personal data in the following circumstances:

1. Where we need to perform the contract we have entered into with you.
2. Where we need to comply with a legal obligation.
3. 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.

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

1. Where we need to protect your interests (or someone else's interests).
2. Where it is needed for official purposes.

How will you use my "Sensitive Personal Data"?

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

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations.
3. Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme, and in line with our data protection policy.
4. Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.
5. Where we need to accommodate any of your specific requirements.

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 employees or former employees in the course of legitimate business activities with the appropriate safeguards.

Our obligations as an employer

We care about the security and integrity of your Personal Data, so we will:

1. Only process your Personal Data in accordance with the Data Protection Regulatory requirements;

2. Perform appropriate due diligence on all suppliers that may come into contact with your Personal Data to provide you with certain benefits;

3. Ensure that there are appropriate technical and organisational security measures in place to protect your Personal Data; and

4. Ensure that all employees are fully trained regarding the appropriate Data Protection Regulatory requirements.

Do we need your consent?

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

In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. 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.

What happens if you don't provide your Personal Data?

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 ensuring the health and safety of our workers).

Change of purpose

We will only use your personal data 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 data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so. Please note that we may process your personal data without your knowledge or consent, in compliance with applicable laws, where this is required or permitted.

How long is mv Personal Data stored for?

Generally, all personal data we collect and process will be retained for seven years from the date of termination of your employment with the Data Controller.

However, wherever possible, we will look to permanently delete any personal data that is no longer required or utilised which means some personal data may be retained for a shorter period if appropriate.

Is my data being transferred to any third party and are they located outside of the EEA? If so, are there appropriate or suitable safeguards in place for this transfer?

We do use third party suppliers to help us provide you with remuneration and other benefits and these suppliers do process your Personal Data. However, please be assured that all of our suppliers go through a thorough process of due diligence to ensure we are satisfied with their levels of security and compliance processes.

We do have third party suppliers that are located outside of the EEA. However, we will always aim to ensure that all suppliers have appropriate contractual safeguards in place prior to any transfer of personal data.

Is my Personal Data being automatically processed in any wav?

For our HR processes we do not have any automated decision-making processes in place.

What rights do I have regarding mv Personal Data?

- **Access**

  You are entitled to request access to any personal data that you wish to have visibility of that we have or may have processed about you.

- **Rectification**
  You are entitled to request that your personal data is rectified or updated if there is any change.

- **Erasure**
  You are entitled to request deletion of any personal data that the company currently holds about you. Please note that this right is not exhaustive and is subject to the Data Controller's legal obligations.

- **Restriction of processing**
  You are entitled to request that your personal data is restricted from being processed .

- **Object to processing**

You are entitled to object to your personal data being processed in a particular way.

- **Data portability**
  You are entitled to request that your personal data is provided to you in a portable manner.

- **Withdrawal of consent at any time (if reliant on consent)**
  Where your consent has been obtained and requested for any particular purpose, you are entitled to withdraw your consent at any time.

- **Automated Decision Making**
  You are entitled to be fully informed of any automated decision-making policy and the factors that impact on this process and how this can be overcome.

- **The right to lodge a complaint with a supervisory authority**
  You are entitled to raise a complaint with the relevant and appropriate Supervisory Authority, namely the Information Commissioners Office, should you have any concerns regarding the processing of your personal data by the Data Controller and feel that you require some form of compensation.

Who is the Data Protection Officer (DPO) and how do I contact them?

Name:	Sadie Brook
Email:	DPO@idhl.co.uk
Office Number:	01423 722061

When should I contact the Data Protection Officer?

Please see Appendix 1

Appendix 1

This appendix is to clarify when you should contact the Data Protection Officer (DPO) and what you can expect to happen after you have reported an incident.

When to contact the DPO?

There are a few instances when you should contact the DPO and these are detailed below:

1. When you wish to make a Data Subject Access Request.
2. When you receive a Data Subject Access Request.
3. When you become aware that there has been an internal Data Incident.
4. When you become aware of an external Data Incident.

What is a Data Subject Access Request?

You may remember from your training that a "Data Subject" is any living individual located within the EEA and a "Subject Access Request" is when that individual makes a request regarding their personal data in relation to any of the following areas:

- Access
- Rectification
- Erasure
- Restriction of processing
- Portability
- Object to Processing
- Automated decision making
- Compensation.

As you correspond with individuals outside of the company it is possible that you may receive a Subject Access Request at any point. In this case you should report it to the DPO via: DPO@idhl.co.uk

Where you wish to make a Subject Access Request for any reason you can email DPO(öidhl.co.uk for this request to be processed. As a reminder, we have 30 days to process any request received.

What is a Data Incident?

A Data Incident is anything relating to any:

- Loss (accidental or otherwise) of personal data
- Destruction of personal data
- Alteration of personal data
- Unauthorised disclosure of personal data

- Unauthorised access to personal data

that is transmitted, stored or otherwise processed.

This can happen with any of your work equipment or it could be the loss of written documentation. Common examples include but are not limited to:

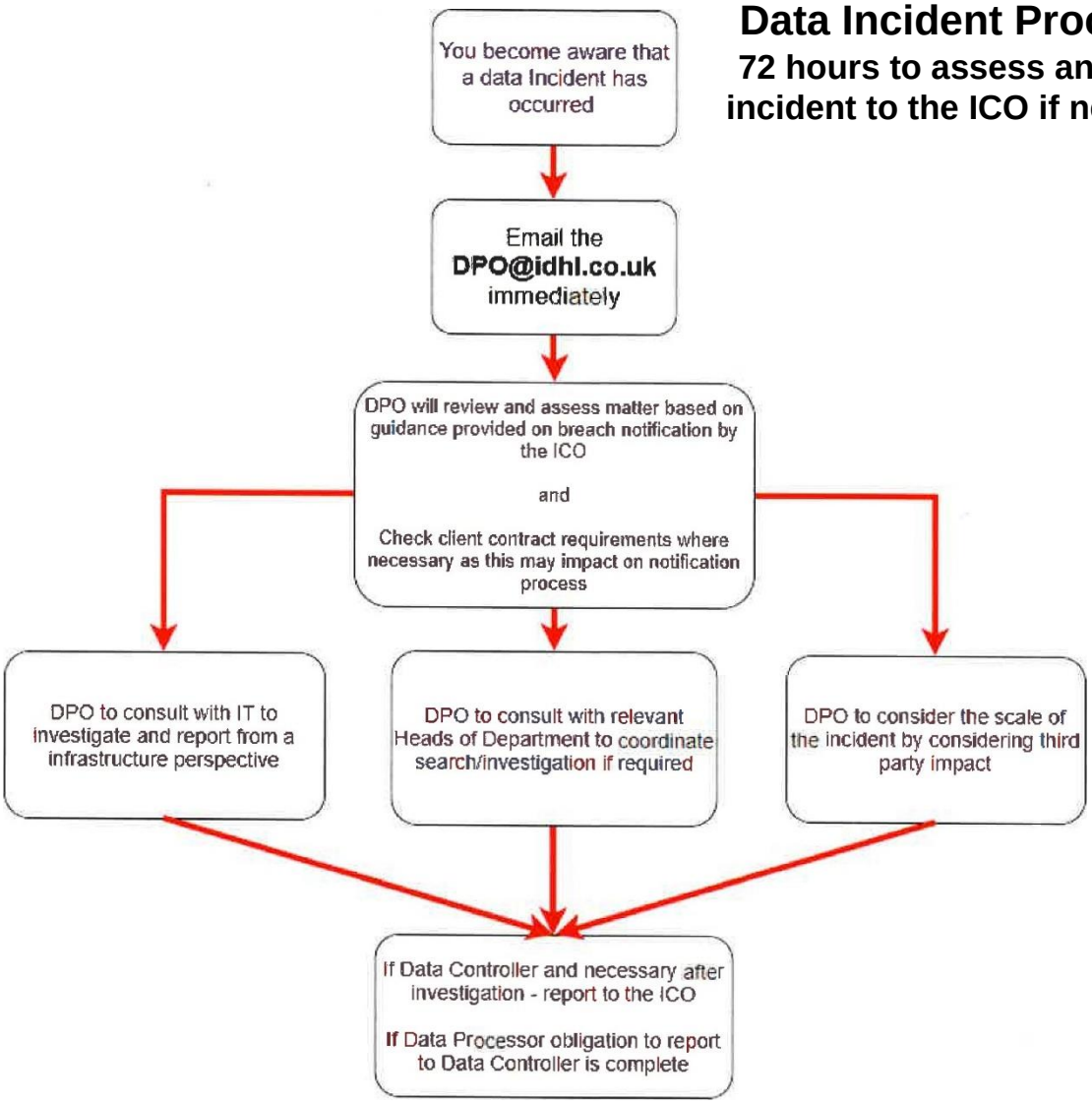
- Loss of data/equipment with personal data on it
- Theft of data/equipment with personal data on it
- Accessing a work account that you do not have permission to access for whatever reason
- Human error such as sending an email to the wrong client or reporting on the wrong client data in a report.
- Any failure of equipment that leads to a loss of data

What happens if I don't report a Data Incident?

Full details are provided in the Data Protection Policy which is available on the IDHL Group's chosen HR Platform from time to time.

What is the process when a Data Incident is reported?

Please see the below flowchart as indication of the process to investigate a Data Incident.



What is the process when a Data Incident is reported?

Please see the below flowchart.

You will see that this does cover direct application of a Subject Access Request as well as what is required if an indirect Subject Access Request is made.