# BHP GDPR Policy

**Introduction**
New regulations for Data Protection came into effect on 25/5/18, specifically called the General Data protection Regulations or GDPR. While financial and commercial operations were a primary focus for these changes, the new regulations do have an impact of BHP. We have therefore compiled a Policy and Action Plan in proportion with what we are required to do under the new regulations.

**Recommendations**
*That the Board considers and approves the Policy and Action Plan below*

# BHP GDPR Policy

## 6 Principles of GDPR

To comply with GDPR, all staff need to embed six privacy principles within their operations:

**1. Lawfulness, fairness and transparency**
Transparency: Tell the subject what data processing will be done.
Fair: What is processed must match up with how it has been described. Lawful: Processing must meet the tests described in GDPR.

**2. Purpose limitations**
Personal data can only be obtained for “specified, explicit and legitimate purposes”. Data can only be used for a specific processing purpose that the subject has been made aware of and no other, without further consent.

**3. Data minimisation**
Data collected on a subject should be “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed”. In other words, no more than the minimum amount of data should be kept for specific processing.

**4. Accuracy**
Data must be “accurate and where necessary kept up to date”. Baselining ensures good protection and protection against identity theft. Data holders should build rectification processes into data management / archiving activities for subject data.

**5. Storage limitations**
Regulator expects personal data is “kept in a form which permits identification of data subjects for no longer than necessary”. In summary, data no longer required should be removed.

**6. Integrity and confidentiality**
Requires processors to handle data “in a manner [ensuring] appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage”.

These 6 principles give a top level overview of the areas covered by the new regulation, however they do not delve into nuances of consent and other articles of GDPR, nor the complexities of data flow mapping, lineage and coordination activities associated with implementing a programme to meet GDPR compliance.

# Your rights as a data subject

As a data subject, you have the following rights under the GDPR, with particular reference to your employment.

1. The right to be informed that we are processing your data. We are confirming this by this letter, and we shall cover this in a separate policy.

2. The right of access to your personal data. You may request a copy of your personal data, and we have one month to provide it, in complex cases, this may be extended to two months.

3. The right to rectification: If we are processing inaccurate personal data about you, you have the right to get it rectified. We have one month to respond, which may be extended to two months in certain circumstances. If we do not respond to your request, we will inform you of that fact, and also of your rights to seek a judicial remedy or go to the Information Commissioner's Office 'ICO'.

4. The right to restrict processing. You have the right to request the restriction of processing of your personal data. This right may be balanced by our right to process data for our legitimate interest.

5. The right to erasure: You have the right to have your personal data erased where it is no longer needed, or, if consent was the basis for us processing it, you no longer consent. In certain circumstances, we may need to keep personal data that you might wish us to erase in connection with possible legal claims (e.g. if there is an accident at work).

6. You have the right to object to data processing where it is based on legitimate interests.

# Photographs and GDRP

The following GDRP laws apply to photographs:

• **The right to be informed (articles 13 and 14)**

You must be clear about the context of how the photos are being used. For example you could not use photos for social media if permission had only been given for printed brochures.

• **The right to access (article 15)**

Individuals have the right to access their personal data (photos) on request, and receive confirmation regarding how these are being used.

• **The right to erasure (article 17)**

Individuals have the right to request photos be removed from websites, social media or future versions of printed materials.

The ICO guidance about taking photographs in schools states "Where the DPA does apply, a common sense approach suggests that if the photographer asks for permission to take a photograph, this will usually be enough to ensure compliance."
It does not state who the photographer must get permission from (parent or teacher), or if indeed this must be in writing. In relation to Media Use it states "A photograph is taken by a local newspaper of a school awards ceremony. As long as the school has agreed to this, and the children and/or their guardians are aware that photographs of those attending the ceremony may appear in the newspaper, this will not breach the DPA."

It is therefore suggested that when confirming an event with a school or group, include a statement similar to that given below:

*The Belfast Hills Partnership would like to take photographs of pupils as part of this event. As we are a charity these photographs will be used to help promote the work we do. Images may be sent to funders as evidence of work undertaken, used on social media pages, the BHP website, printed brochures, reports or in presentations. Before taking photographs staff will also check with both leaders and young people if they are happy to have their photograph taken.*

*Individuals can contact us about how their photograph has been used and we are happy to remove any images from websites, social media or future versions of printed materials. If you have any further questions or concerns please do not hesitate to get in touch.*

In terms of child protection (as opposed to GDRP) some general advice is to take a picture of the whole group as opposed to focus in on an individual pupil. Not to name the young person or their school, and avoid clear images of school logos to help ensure the child's safety.

# Data Protection Policy for Employees

This policy does not form part of employees' terms and conditions of employment and may be subject to change at the discretion of management.

In the course of your work you may come into contact with and use confidential personal information about people, such as names and addresses or even information about customers' circumstances, families, health and other private matters.

This policy helps you ensure that you do not breach the Data Protection Act 1998, the GDPR or the Data Protection Act 2018 (when in force), which all set strict legal standards in this area, for simplicity we refer to them in here as 'the Data Protection Act'. If you are in any doubt about what you may or may not do, seek advice from your Line Manager. If you are in doubt and cannot get in touch with him/her or a manager or director responsible for Data Protection, do not disclose the information concerned.

The Company holds personal data about you. In your employment contract you have consented to the data being used as set out in the contract. If this information changes, you should let us know so that our records can be updated.
These records may include:

- Information and references collected during the recruitment process.
- Details of terms and conditions of employment, including pay and benefits, your age and qualifications.
- Payroll, tax and NI information.
- Performance information.
- Details of grades and job duties.
- Health records.
- Absence, self-certification forms and holiday records.
- Details of disciplinary investigations and proceedings.
- Details of grievance investigations and proceedings.
- Minutes from meetings attended.
- Details of expenses and travel.
- Accident records.
- Training records.
- Contact and next of kin details.
- Information collated to ensure compliance with legislation and monitoring of equal opportunities compliance.
- Correspondence with the Company and other information provided to the Company.
- Details of websites visited using company-provided internet access, emails and messages sent and received and other correspondence, and work-related social media, e.g. LinkedIn.
- Data generated in relation to your location, use of electronic devices and travelling.
- Photographs and pictures of you.
- Work related social media, e.g. LinkedIn

The Company believes these uses are consistent with the employment relationship and with the principles of the Data Protection Act. The information held will be

principally for our management and administrative use only. Occasionally we may need to disclose information about an employee to relevant third parties, e.g. when legally required to do so or when managing the employment relationship, e.g. processing payroll, managing HR, in connection with legal claims, managing holidays and attendance, and managing health and safety matters.

The Company might need to hold further information on employees but disclosure to any other person will be made only when strictly necessary for the following purposes:

- Regarding an employee's health, for the purpose of compliance with our health and safety and our occupational health obligations. To assist with management decisions relating to whether an employee's health affects their ability to do their job, whether reasonable adjustments are necessary to assist employee's with a disability.
- For the purpose of insurance, pension, sick pay and other related benefits in force from time to time.
- In connection with unspent convictions to enable the Company to assess and employee's suitability for employment.

The Data Protection Act 1998 requires that eight data protection principles be followed in the handling of personal data. These are that personal data must:

- be fairly and lawfully processed;
- be processed for limited purposes and not in any manner incompatible with those purposes;
- be adequate, relevant and not excessive;
- be accurate;
- not be kept for longer than is necessary;
- be processed in accordance with individuals' rights;
- be secure; and
- not be transferred to countries without adequate protection.

If you access another employee's records without authority this will be treated as gross misconduct and is a criminal offence under s.55 of the Data Protection Act 1998. Other provisions such as the GDPR and the Data Protection Act 2018 will also apply in due course, as detailed later.

On e-mails and faxes, see also the Company internet and e-mail policy but also follow the guidance below recommended by the Information Commissioner's Office.

The Company follows the retention periods recommended by the Information Commissioner in its Employment Practices data protection code of practice.

You should therefore treat the following as guidelines for retention times in the absence of a specific business case supporting a longer period.

| | |
|---|---|
| Application form | Duration of employment |
| References received | 1 year |
| Payroll and tax information | 6 years |

| | |
|---|---|
| Sickness records | 3 years |
| Annual leave records | 2 years |
| Unpaid leave/special leave records | 3 years |
| Annual appraisal / assessment records | 5 years |
| Records relating to promotion, transfer, training, disciplinary matters | 1 year from end of employment |
| References given/information to enable references to be provided | 5 years from reference/end of employment |
| Summary of record of service, e.g. name, position held, dates of employment | 10 years from end of employment |
| Records relating to accident or injury at work | 12 years |

Any data protection queries should be addressed to your line manager or any data Protection Officer.

## The bases for the Company processing your personal data

As a data controller, we have to have a lawful basis or bases for processing your personal data, and have to inform you of the fact that your data is being processed. The Company processes personal data on the following bases:

1.For the performance of a contract (i.e. your contract with us). We process data relating to your name and address, your bank or payroll details, your pay information in order to pay you (and to make permissible deductions from your pay), working hours, holidays and other aspects of your personal data to enable us to perform our obligations to you under your contract, and to monitor your obligations to us.

2.In order to comply with legal obligations: We may process your data in order to make deductions from your pay, e.g. to ensure that HMRC receive the income tax and National Insurance due on your earnings, where we have to disclosure information required by law, e.g. a court order, for health and safety compliance, or otherwise where disclosure is mandatory (e.g. in the event of a business transfer, specified personal data of certain employees may have to be disclosed to the new employer)

3. For the protection of our legitimate interests: We process your personal data to ensure that our legitimate interests in running our operations in an efficient manner and in compliance with the law means that we may have to process personal data about you including data about your whereabouts, time keeping, conduct, to conduct disciplinaries and grievances, to ensure that we maintain a safe working environment, to ensure that we comply with our obligations in respect of equal opportunities and to establish, present and defend legal claims or to seek advice on handling situations, to provide employment references, to keep training records, details of employee performance, driving licences (where applicable), use of vehicles in connection with your employment, data from any CCTV used in relation to our activities, records of any drug or alcohol testing undertaken records of criminal convictions that may impact on your employment, details of health where capability for employment or safety may be an issue, and details of disabilities in order to comply with our obligations to disabled

employees. We may also process certain data around recruitment and appointments under this basis.

4. Where it is necessary to protect vital interests: We may need to keep and process data on next-of-kin contact details and any particular medical conditions of employees, or your whereabouts, or work-related travel in order to ensure that your vital interests are protected in the event of an emergency.

5. We process data on the basis of consent where you agree to it, for example, if you agree to provide consent to a medical report, or with internal job applications.

# List of Personal Data Held by the Belfast Hills Partnership

Numbers – database
Letters – where they are stored

1. Staff personal contacts
a. Mobile phones
b. Email contacts
2. Board members
a. BHP Board Docs
b. ADMINISTRATION – BHP Contacts
3. Friends List
a. Friends Membership
4. Staff Info
a. Sage Payroll
b. Info folder in JB office
5. Other Contacts
a. BHP Contacts Directory
b. ADMINISTRATION
c. WCP Volunteer Wardens
d. Belfast Hills Society contacts
e. LPS Volunteer Contact Details
f. Archaeology Dig Bookings
g. Geology Course Bookings
h. Undergraduate Skills Applicants
i. Heritage Festival Bookings
j. Schools

# Reporting an Incident

## 1. Introduction

In accordance with The General Data Protection Regulation (GDPR) 2018, the Data Protection Act 1998, The Data Protection Directive 1995, and associated Data Protection legislations, Northern Ireland Environment Link shall document all data incidents immediately as they occur.

This form is for reporting data incidents. The incident reporter should fill in sections 2, 3, 4, 5. It is important that as much detail as possible is recorded whilst this is fresh in the minds of the individuals involved to ensure an accurate and thorough record is maintained. These records may be required to demonstrate Belfast Hills Partnership's response to a data incident internally and where applicable with Data Protection Authorities and/ or clients.

This procedure is applicable to BHP and encompasses all personal data held and used by BHP internally and on behalf of our partners and clients.

## 2. Reporting Person Details

| | |
|---|---|
| **Name** | |
| **Email** | |
| **Phone Number** | |
| **Job Title/Role** | |

## 3. Data Details

It is important that the data involved in the incident is identified

| | |
|---|---|
| **Common name for data type** | |
| **Record Type** | |
| **Format/s of Data** | |
| **Personal Data Content** | |
| **Data Owner (Client, BHP, other)** | |
| **Client/s Name (if applicable)** | |
| **Client contractual country of governing law** | |
| **Nationality/s of dataset (eg UK)** | |

## 4. Incident Timeline

Dates and times must be as accurate as possible. Where these are a best guess this must be noted as an estimate or have the known window of times and/ or dates detailed.

| | Date | Time |
|---|---|---|
| **Occurred** | | |
| **Discovered** | | |
| **Reported** | | |

## 5. Incident Details

Please provide as much detail as possible

| | |
|---|---|
| **What occurred** | |
| **How did the incident occur** | |
| **Why did the incident occur** | |
| **Individuals involved in each stage** | |
| **Identify technology, hardware, software, platform, file share locations etc involved** | |
| **Relevant process, policy or documents** | |
| **What was the incident** (E.g. loss of data, accidental disclosure or destruction of data, breach of rule, excessive privileges or access control failure, compromise of information, natural disaster, physical damage, infrastructure, technical failure, malware, technical attack, programming issue, process oversight etc) | |
| **How was the incident detected** | |
| **How long had the incident lasted** | |
| **Immediate corrective action taken** | |
| **Are client/s aware of the incident** | |
| **What exactly has client/s been exposed to & what are perceptions** | |
| **Known relevant client contract terms** | |
| **Any other details** | |

## 6. Corrective & Preventative Action

The following section should be completed in conjunction with the designated staff member responsible for data protection and the relevant line manager.

| | Corrective & Preventative Action |
|---|---|
| **Overview** | |
| **Client** | |
| **Process** | |
| **Development, software etc** | |
| **Hardware, technology etc** | |
| **BHP training & education** | |
| **Record keeping: Action completed, controls & audit trail** | |
| **Internal communication to take place** | |
| **External communication to take place** | |
| **Incident Response Authorized** | |
| **Incident Closed** | |
| **Report shared with Management** | |