Group Privacy Policy Statement

1. The Controller - Who we are:

Ballyvesey Holdings Limited. Please consult document "Trading Companies" for individual entities.

2. Data Protection:

Data Protection in the Ballyvesey Divisions is administered by the GDPR Steering Committee.

- James Darragh (Compliance & HR)
- Gordon Willis (ICT)
- David Andrews (Chief Information Officer)

All members of the GDPR Steering Committee have received training on data protection and information security relating specifically to their responsibilities. In addition, at least one member of the Steering Committee holds a General Data Protection Regulations Practitioner Certificate.

The Steering Committee can be contacted by emailing: dataprotection@ballyvesey.com

Or by writing to:

Data Protection, Ballyvesey Holdings Limited, 607 Antrim Road, Newtownabbey, BT36 4RF

3. Lawfulness and Compliance:

Ballyvesey Holdings Limited undertakes to protect the rights and freedoms of all individuals whose data we process. We will uphold the principles in Article 5 of the General Data Protection Regulations 2016, as directed by the European Court of Justice and when applicable, the rights provided under statute by any Act of Parliament having gained Royal Assent including the Data Protection Act 2018, and any Amendment Bills or future Bills thereof. We recognise the authority of the Information Commissioner's Office, the Surveillance Commissioner's Office, the Police Authorities of the United Kingdom and Northern Ireland, the Criminal Records Bureau, The Health and Safety Executive, HM Tax Inspector's Office and any other competent authority where they have relevance in these matters.

We acknowledge that the only law repealed by the General Data Protection Regulation 2018 is the Data Protection Act (UK) 1998 and that any other law introduced, or not repealed alongside this Regulation must also be recognised with equal authority, insofar as it has not been read down by any court of law to provide protection of the rights and freedoms conferred by the Regulation.

4. How we gather personal data:

Throughout the Group information is gathered in the normal course of business. The information we collect may include Public Data, Company Data, Third Party Data and Personal Data. Personal Data is protected in law by the General Data Protection Regulations EC 2016/679 and the Data Protection Act (UK) 2018. Where personal data is collected or provided to us a relevant privacy notice will be available summarising the following:

- who we are
- who deals with our data protection
- our purposes and legal basis for processing the personal data
- our legitimate business interests in processing the personal data
- who we may provide the personal data to
- whether we transfer the personal data to another member state, or international country
- the length of time we will keep the personal data
- a summary of your rights and freedoms to the processing of your personal data
- what may happen if you fail to provide / withdraw / object to the processing of the personal data, whether or not we process any personal data by automated means, including profiling individuals, or the existence of any monitoring of individuals.

Sources of personal data can come from individuals themselves, be provided to us by a third party where you have previously agreed the legitimate interest to do so, be obtained from public records, or a competent authority.

5. **Why we need personal data:**

Most often personal data will be needed along with other information to allow the group to operate according to its legitimate business interests. Other times we are required to process personal data to comply with a legal obligation, or to fulfil the requirements of a legally binding contract already in place, or that we may intend to enter into. Our business model has no intended processing in the public interest, unless a situation may occur which would morally require us to do so, for example to comply with the Whistle Blowing Policy, or the Modern Day Slavery Act. In an individual's vital interests, we may make a disclosure in an emergency where we believe they may be in threat of life or serious harm. Where processing is based on consent, we will obtain that consent and keep a record of doing so; you will have the right to withdraw your consent at any time, but this will not affect the legal standing of the processing that occurred prior to you exercising this right.

6. **Fairness and Transparency:**

We will process personal data fairly and with transparency to the individual who owns the personal data. We acknowledge the right of an individual to submit a Subject Access Request for any personal data which we hold about them. We will advise individuals if we transfer their personal data to a previously un-notified organisation to process in the business interests. We will notify any affected individuals of a breach if we have suffered a theft, destruction or other loss of their personal data as soon as the facts are fully known and co-operate with ICO, whilst complying with the Regulation.

7. **Purpose Limitation:**

We will process personal data for the purposes which we have stated. If we need to process personal data for a new lawful purpose we will be transparent and fair about this process.

8. **Data Minimisation:**

We will restrict collection of personal data to that which we really need. We will not ask for any information which is unnecessary. Once personal data is no longer necessary we will responsibly destroy it, or return it to the individual who owns it. Where retention of data is required without the need to retain the personal data alongside it, we will use personal data anonymization and pseudonymisation to remove or disguise the personal element of the data.

9. **Accuracy:**

We will take every reasonable step possible in the good practice of due diligence to ensure the accuracy of any personal data which we hold or process. Compliance checks, system auditing and staff training are carried out in order to minimise the risk and / or impact of inaccuracy in data generally. Where the personal data we hold is found to be incorrect an individual owning the personal data can request that we correct, rectify, erase or withhold it.

10. **Storage Limitations:**

Personal data will only be retained for as long as it is necessary and where we have a legitimate business purpose, or a legal obligation to do so. If we are found to hold personal data unjustifiably the individual who owns the personal data can ask us to return, erase, or destroy it. A retention policy forms part of any privacy notice available when personal data is collected.

11. **Integrity and Confidentiality:**

We will store and process personal data with the appropriate security and protect it from unauthorised or unlawful processing, accidental loss, destruction, or damage, as far as we possibly can, using appropriate and technical measures.

We train our employees with different levels of data protection and information security protocols appropriate to their job roles. The group use robust usage policies as part of the terms and conditions of employment and use investigative and disciplinary procedures to enforce compliance with these policies throughout all levels of the workforce. Background checks and references are sought from new employees, in addition to a requirement for them to prove their identity. Wherever possible we try and obtain a copy of a passport of new employees to prove their identity, or otherwise another document to ensure their right to work within the UK and reduce the risk of modern slavery by requiring the employee to be in possession of their own passport in a safe environment. Records will be kept of identity documents, references and qualifications to demonstrate compliance with the regulation.

Employees are required to practice a clear desk policy and lock screens when away from their computer. Group policy controls and login permissions are used to restrict access to relevant areas of software. Password enforcement is used to ensure complexity and frequent changing of passwords. Employees' requirements to remotely access systems with a work laptop from home or another location are subject to risk assessment based on needs, training and risks. If granted, remote access is through a Virtual Private Network (VPN) encrypted end to end using 256 bit technology. Employee permissions can be restricted or revoked if abused and access to systems removed completely when an employee leaves the group.

Electronic systems throughout the Group use our own servers located in premises owned by the Group. Backup systems shadow and mirror the live service in alternative locations and can be switched over with minimal effort as part of our disaster recovery plan (DRP). A DRP is in place for all electronic systems and its deployment is under the control of the GDPR Steering Committee, at least one Member of which has direct authority over our IT systems. Electronic Systems are supported by our internal ICT division which forms an integral part of the Group. Support is provided by a team of professionals both within a dedicated ICT control room and field operatives in situ at locations throughout the Group.

In addition to physical security present at hosting and support locations, access to premises is controlled by coded doors and / or swipe systems including biometrics at selected points. All server rooms are secured with appropriate locking mechanisms. Systems are monitored by multi-layer firewall protection, anti-virus systems, access control systems, and Group Policy settings. Incoming and outgoing mail is monitored and filtered, access to USB ports restricted, redundant hardware including drives are stored securely until dismantled and destroyed.

Portable devices such as laptops, tablets and smartphones are encrypted, secured with pins and passwords and anti-loss technology.

Physical files containing personal data are kept in locked areas, in fire resistant cabinets with restricted access. Any confidential waste records containing personal data are placed in locked letterbox bins until they can be shredded. Shredding is regularly carried out on site by a security cleared contractor under strict conditions.

12. **Controllers and Processors:**

Any division within the Group processing personal data at the point of contact is a "Data Controller"

Any division within the Group sharing personal data, or accessing shared personal data within the group is a "Controller in Common"

Any division within the Group processing personal data on behalf of another division within the group is a "Data Processor"

Any party processing personal data on behalf of any division within the group, if in itself it is not part of the group, then they are a "Third Party Processor"

Where a third party processor is used, individuals to whom the personal data belongs will be informed that their information has been provided to the third party. If this action is underpinned by a legal obligation or a legitimate business interest, then consent is not required, providing that adequate safeguards are in place to ensure the processors meet the required compliance of the GDPR. As part of the adequate safeguards, the group requires all third party processors to enter a legally binding contract to ensure compliance with GDPR and protection of the rights and freedoms of the individuals, to whom the original personal data belongs. Any Controller – Processor contract is in addition to any other Service Level Agreement in place (SLA).

13. **Review Policy:**

The GDPR Steering Committee meets at regular intervals of at least once per calendar month, or more often if needed. Any current business is dealt with at that time. Reviews of policies and procedures are part of the normal business of the Steering Committee's activities and they continue to make improvements as required to maintain compliance with all regular laws.

14. **Rights and Freedoms:**

Individuals have the right of subject access to, and to be provided with a copy of, any personal data we hold. This request can be made using contact information provided at point 2 above. It must provide enough information to identify the data subject and satisfy the Controller (us) of the

applicant's identity. Sufficient information to the specific nature of the request, and if known, the location of the information, should be made clear in the content to avoid any unnecessary, disproportionate effort in providing the personal data. We will then be required to respond within one month.

If the subject believes that the personal data we hold is incorrect, they can ask us to rectify it. Proof may be required to enable us to do this, otherwise a note may only be added to state that the information is in dispute.

If the subject believes that we should not have the personal data, because it is unnecessary, beyond the agreed retention period, or that the data has been unlawfully processed or obtained, then they can ask us to erase or return the personal data.

Where any personal data is processed based on the reliance of consent and no other legitimate purpose can be justified, then the subject can withdraw their consent for any future use of the personal data.

If an individual is unhappy about the way the GDPR Steering Comittee deal with their rights and freedoms they can complain in writing to:

Chief Executive Officer
Ballyvesey Holdings Limited
607 Antrim Road
Newtownabbey
BT36 4RF

The Chief Executive Officer or his nominated deputy will carry out an investigation and review of the circumstances and advise them of the findings along with any recommended actions within one month.

If the individual is still unsatisfied with the response of the Company Secretary, or in fact at any other prior stage of the process, they can submit a report to the Information Commissioner's Office.

DPPOLSTMT81024091