1 Purpose

1.1 To govern the handling of personal data processed throughout the Ballyvesey Group and its subsidiaries via centralisation of data protection controls through the Data Protection Committee (DPC).

1.2 To assist Senior Management in ensuring compliance with Data Protection Legislation via a centralised support, provided by the Data Protection Committee (DPC).

2 Scope

2.1 Primary scope – for Group Divisional Leads Company MDs and GMs to ensure compliance with necessary policies and procedures throughout their staff and business operations.

2.2 Secondary Scope – for all employees to understand their responsibilities in processing of personal data.

3 Responsibilities

Oversight	- BVH Board
Governance	– DPC
Compliance	– MDs and GMs
Duties	– All Employees

4 Definitions

4.1 DPC – The Data Protection Committee. A central services committee responsible for governance and policy development in data protection issues.

4.2 DPA – The Data Protection Act 2018 UK Legislation

4.3 GDPR – The General Data Protection Regulations EU Document 2016/679 of the European Parliament and Council 27th April 2016, enforced 24th May 2018.

-or-

The General Data Protection Regulations (UK) 2020, as a consequence of Brexit enforced from 1st January 2021.

4.4 PECR – The Privacy of Electronic Communications Regulations 2003

4.5 DPIA – Data Protection Impact Assessment. A method of risk assessing new procedures that present a novel risk to current data protection processing policies, to ensure that any appropriate steps are taken as necessary to remain compliant with legislation.

4.6 Data Controller – The entity responsible for collection and processing, or use of personal data, having a legitimate interest, or purpose in doing so.

4.7 Data Processor – The entity to which personal data is provided for a specific and explicit purpose, to conduct processing of that data within the terms as agreed to by the controller, or what purposes the controller were advised of when providing the processor with the data.

5 Policy and Procedure

5.1 All staff must undertake relevant Data Protection training, according to their job role. This should include a basic understanding of GDPR and DPA legislation, what it means for them, their employers and the data subjects within their scope.

5.2 All staff must, in good conscience, behave in a responsible manner towards personal data, taking all reasonable steps available to them to ensure safe handling of personal data and compliance with GDPR, DPA, PECR.

5.3 All senior management must to the extent reasonably within their power, ensure that compliance is upheld by the staff under their control. Including but not limited to, creating additional company level controls and policies to ensure that unique, or varied circumstances within their particular business model remain compliant with GDPR, DPA, PECR. The DPC's advice should be sought in drawing up and approving such documents.

5.4 Processing of all personal data must fall within the scope of current policy and be compliant with GDPR, DPA, PECR. Any novel concepts, or new procedures introduced must undergo a DPIA to ensure that they sit within the current policies, otherwise additional controls and policies may need to be introduced. The DPIA must involve the co-operation and support of the DPC.

5.5 All requests for access to personal data must be tightly controlled. Any 3rd party requesting personal data, including supervisory authorities, like the police, must be advised to make their request to dataprotection@ballyvesey.com No employee should engage in conversation with a 3rd party when data protection is evident.

5.6 Video footage, including CCTV and Vue Cameras etc may contain images of individuals' faces. This is biometric data, as your face is unique to your identity. Biometric data falls under special category rules in GDPR and DPA and therefore has further restrictions, than some other items of personal data. All requests for video footage of any kind, for any reason, regardless of by whom it is requested, must be passed to and approved by the DPC.

5.7 Breaches of data protection should be reported to the DPC immediately once discovered. These include unlawful disclosure of, theft of, loss of, destruction of personal data etc. Disciplinary action remains within the remit of relevant line management, the DPC is mainly interested in remedial action, to prevent a reoccurrence, maintaining the security of and the control of the data.

6 Help & Escalation

6.1 In addition to the governance of data protection, the DPC also provides help and support to anyone needing advice, or guidance.

6.2 Any employee unsure of whether an action, or request falls within the scope of data protection ought to in the first instance speak to their line management.

6.3 As a matter of escalation, if the line manager is unsure of the scope of an action, or request, they should escalate to company senior management.

6.4 If company senior management are unsure of the scope of an action, or request, they should escalate to DPC.

6.5 DPC escalation is to the BVH Board via James Darragh as a conjoint board member and DPC panellist.

6.6 Any employee can escalate to the DPC immediately if they believe that to be a necessary course of action.

6.7 At any time in the escalation process that a 3rd party request is identified, then that should immediately be a referral of the requestor to the DPC.

7 DPC Membership

James Darragh	(Legal and representative of BVH Board)
Dave Andrews	(Legislation, policy and compliance)
Gordon Willis	(Cyber and network security)
Darren Ward	(ICT support and systems admin)

8 References

8.1 The legal basis on which a controller is allowed to process data can be found in Article 6 of GDPR.

8.2 The additional basis for special category data can be found in Article 9 of GDPR.

8.3 Attempting to obtain access to personal data without the controller's consent, including by deceit, or omission, is an offence under Section 170 of the Data Protection Act.

8.4 Supervisory authorities, like police, HMRC, customs officials etc have an exemption to process personal data without fear of GDPR under Schedule 2 of the Data Protection Act. However, that exemption comes with conditions that the processing is necessary and not excessive, nor does it remove another statutory right or freedom of an individual affected by it. This exemption only applies to the supervisory authority itself and does not extend to the controller, or their reasons for disclosing the personal data to the supervisory authority.

9 Endorsement

9.1 This policy has been agreed at group level and comes into immediate effect throughout the entire holdings.

Document Control

The Data Protection Committee is the document owner and responsible for ensuring this policy remains current and up to date.

A current version of this document is available to all members of staff on the Security and Governance SharePoint site and is published by the Security and Governance function.

This policy was approved by the Data Protection Committee and is issued on a version-controlled basis.

Representative of the DPC signature:  Date: 13/02/2024

Change History Record

Issue	Description of Change	Date of Change
1.0	Initial Issue	