Ivybridgelink
General Data Protection Regulations and Data Management Policy

IvybridgeLink is a charity set up to provide services to the community at the Bridgelink Centre. It is our policy to provide and maintain safe and healthy working conditions, equipment and systems of work for all staff and volunteers which includes . Where appropriate, we will provide guidance to our clients (being the lessees and end users of our facility) to safely use the Bridgelink Centre.

Data Management Policy

Introduction

IvybridgeLink needs to gather and use certain personal information about the individuals and Centre Partners who use the BridgeLink Centre**.**

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the Project Company's data protection standards and comply with the law.

Why this policy exists

This data protection policy ensures **IvybridgeLink**:

- Complies with data protection law and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Scope

The **IvybridgeLink** does not have any employees, but all contractors, consultants and partners must follow this policy. Generally, this policy refers to anyone **IvybridgeLink** collaborates with or acts on behalf of **IvybridgeLink** and may need occasional access to data.

This Policy applies to all data that the **IvybridgeLink** holds relating to identifiable individuals, even if that information technically falls outside of the General Data Protection Regulation. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Any other personal information relating to individuals, such as helpdesk records

Data Protection Officer

IvybridgeLink's 'core activities' do not require regular and systematic monitoring of data subjects on a 'large scale', nor do they involve 'large scale' processing of 'special categories' of personal data and relating to criminal convictions and offences. Therefore, it does not have a dedicated Data Protection Officer (DPO).

Policy Elements

In order to offer services to the community at the BridgeLink Centre**, IvybridgeLink** needs to obtain and process information. This information may include any offline or online data that makes a person identifiable such as names, addresses, usernames and emails addresses, photographs etc.

IvybridgeLink collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to **IvybridgeLink**, the following rules apply.

IvybridgeLink data will be:

- Accurate and kept up to date
- Collected fairly and for lawful purposes only
- Processed by the company within its legal and moral boundaries
- Protected against any unauthorized or illegal access by internal or external parties
- Securely stored and password protected

IvybridgeLink data will not be:

- Communicated informally
- Stored for more than a specified amount of time
- Transferred to organizations, that do not have adequate data protection policies
- Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)
- Stored on local machines or external removable hard drives

In addition to ways of handling the data the **IvybridgeLink** has obligations towards the people to whom the data belongs. Specifically, **IvybridgeLink** must:

- Inform people know what data is collected
- Inform people about how data is processed
- Inform people about who has access to their information
- Have provisions in cases of lost, corrupted or compromised data
- Allow people to request that we modify, erase, reduce or correct the data we hold, in accordance with the General Data Protection Regulation.

Actions

To exercise data protection **IvybridgeLink** is committed to:

- Restrict and monitor access to sensitive data
- Develop transparent data collection procedures
- Train employees in online privacy and security measures
- Build secure networks to protect online data from cyberattacks
- Establish clear procedures for reporting privacy breaches or data misuse
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.)

- Report any data loss or breaches to the **IvybridgeLink** Board of Trustees within 72 hours of discovering a data breach, as this may need to be reported to the Information Commissioner's Office.

Change Record

Date of Change:	Changed By:	Comments:
25/3/24	Katherine Morgan	Sent to DS for annual review
12/07/25	Katherine Morgan	Sent to DS for annual review in September
15/09/25		To be reviewed at meeting by trustees