Listening and learning from the next generation

Data Protection Guidelines

Silver Lined Horizons needs to gather and use certain information about individuals.

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

Personal data is data held about an identifiable living person. Data we hold about children, young people and adults includes but is not restricted to: Name; address; date of birth; guardian contact details; email address; phone number.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection and privacy standards – and to comply with General Data Protection Regulation (GDPR).

Who we are references to we, our or us in these guidelines

• Silver Lined Horizons (SLH) incorporated and registered in England and Wales with company number 08229102, whose office is at 3 Blakes Ave, New Malden, KT3 6RJ. SLH is registered with the Information Commissioner's Office as a Data Controller – registration number ZA335759

• Chateez (registered trademark of SLH)

Why this policy exists

The data protection policy ensures Silver Lined Horizons:

- Complies with GDPR and follows 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

General Data Protection Regulation (GDPR)

GDPR describes how organisations – including Silver Lined Horizons – must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

General Data Protection Regulation (**GDPR**) is underpinned by six privacy principles which we set out to embed within our operations:

1. Lawfulness, fairness and transparency
2. Purpose limitations
3. Data minimisation
4. Accuracy
5. Storage limitations
6. Integrity and confidentiality

People, risks and responsibilities

Policy Scope

This policy applies to:

- All staff and volunteers of Silver Lined Horizons
- All contractors, suppliers and other people working on behalf of Silver Lined Horizons

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside GDPR. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- …plus any other information relating to individuals

Data protection risks

This policy helps to protect Silver Lined Horizons from some very real data security risks, including:

- **Breaches of confidentiality**. For instance, information being given out inappropriately
- **Failing to offer choice**: For instance, all individuals should be free to choose how the company uses data relating to them.

- **Reputational damage**: For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Silver Lined Horizons has some responsibility for ensuring data is collected, stored and handled appropriately.

Data storage

These rules describe how and where data should be safely stored.

- When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it.
- These guidelines also apply to data that is usually stored electronically but has been printed out for some reason.
- When not required, the paper or files should be kept in a **locked drawer or filing cabinet**.
- Employees should make sure that paper and printouts are not left where **unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- All personal data about young people and their views must be kept secure. This means:
- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD) these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service.
- Servers containing personal data should be sited in a secure location.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- All servers and computers containing data should be protected by approved security software.

Data retention

Please see separate documentation and retention disposal policy for further information on data retention periods.