# Data protection policy

**Our Data Protection Policy sets out our commitment to protecting personal and student data and how we implement that commitment with regards to the collection and use of personal data.**

---

## Commitment:

We are committed to:

- Ensuring that we comply with the eight data protection principles, as listed below.
- Ensuring that data is collected and used fairly and lawfully.
- Processing personal and student data only in order to meet our operational needs or fulfill legal requirements.
- Taking steps to ensure that personal and student data is up to date and accurate.
- Establishing appropriate retention periods for personal and student data.
- Ensuring that data subjects' rights can be appropriately exercised.
- Providing adequate security measures to protect personal and student data.
- Ensuring that a **nominated officer** is responsible for data protection compliance and provides a point of contact for all data protection issues.
- Ensuring that all staff are made aware of good practice in data protection.
- Providing adequate training for all staff responsible for students and personal data.
- Ensuring that everyone handling student and personal data knows where to find further guidance.
- Ensuring that queries about data protection, internal and external to the organization, are dealt with effectively and promptly.
- Regularly reviewing data protection procedures and guidelines within the organization.

---

## Data Protection Principles:

1. Personal and student data shall be processed fairly and lawfully.
2. Personal and student data shall be obtained for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with those purposes.
3. Personal and student data shall be adequate, relevant, and not excessive in relation to the purpose for which they are processed.
4. Personal and student data shall be accurate and, where necessary, kept up to date.
5. Personal and student data shall not be kept for longer than necessary for the purposes for which they were processed.

6. Personal and student data shall be processed in accordance with the rights of data subjects under the Data Protection Act.
7. **Appropriate technical and organizational measures shall be taken against unauthorized and unlawful processing of personal and student data and against accidental loss, destruction, or damage of personal data.**
8. Personal and student data shall not be transferred to a country or territory outside unless that country ensures an adequate level of protection for the rights and freedoms of data subjects.

---

## Managing Data Security Breaches:

**Introduction:**
In the event of a data security breach, SAFETY HOUSE is committed to managing the breach in a prompt, effective, and transparent manner to minimize risks to individuals and safeguard the integrity of our data systems.

**Breaches Covered:**

- Unauthorized access to personal or student data.
- Accidental loss, destruction, or theft of data.
- Data being disclosed to an unauthorized individual or organization.
- Unauthorized alteration or destruction of data.
- Compromise of data systems through hacking or malicious software.

---

## Steps for Managing Data Security Breaches:

1. **Breach Detection and Reporting:**
    - Any staff member or third party who becomes aware of a potential data breach must immediately report it to the **Data Protection Officer**.
    - The breach report should include:
        - Date and time the breach was detected.
        - Description of the nature of the breach.
        - Type of data compromised.
        - Initial assessment of the scope and potential risks.

2. **Containment and Recovery:**
    - The **Data Protection Officer** will immediately take steps to contain the breach and prevent further data loss or exposure.
    - Depending on the nature of the breach, containment may involve:
        - Disabling compromised systems.
        - Securing access points.
        - Isolating affected networks.
    - The **Data Protection Officer** will work with IT support and other relevant departments to recover any lost data, restore system integrity, and ensure that any vulnerabilities are resolved.

3. **Risk Assessment:**
    - The **Data Protection Officer** will conduct a thorough risk assessment of the breach, which will include:
        - Identifying the scope of the breach and the type of data affected.
        - Assessing the potential impact on affected individuals (e.g., financial loss, identity theft, reputation damage).
        - Estimating the likelihood of further exposure or harm.

4. **Notification to Affected Parties:**
    - If the breach is likely to result in a high risk to the rights and freedoms of individuals, SAFETY HOUSE will notify the affected individuals without undue delay.
    - Notifications will include:
        - A description of the nature of the breach.
        - The actions being taken to address the breach.
        - Recommendations for the affected individuals to protect themselves from further harm (e.g., changing passwords, monitoring for suspicious activity).
        - Contact details of the **Data Protection Officer** for any further queries.

5. **Notification to Supervisory Authorities:**
    - If the breach meets the criteria for reporting under the relevant data protection regulations (e.g., GDPR), SAFETY HOUSE will notify the appropriate supervisory authority (e.g., the Information Commissioner's Office) within **72 hours** of becoming aware of the breach.
    - The notification will include:
        - The nature of the breach and the data affected.
        - Steps taken to contain and mitigate the breach.
        - Any further actions planned or underway to prevent recurrence.

6. **Review and Remediation:**
    - After the breach has been contained and risks mitigated, SAFETY HOUSE will conduct an internal review to identify the root cause of the breach and determine whether any changes to processes, systems, or training are required.
    - A formal report will be prepared, outlining:
        - The details of the breach.
        - The containment and recovery actions taken.
        - The lessons learned and recommendations for improvement.
    - The report will be reviewed by senior management, and any necessary changes will be implemented promptly.

7. **Staff Training and Awareness:**
    - SAFETY HOUSE will ensure that all staff are regularly trained on data protection and data breach procedures.
    - Refresher training will be conducted following any significant breach to reinforce best practices and reduce the risk of future incidents.

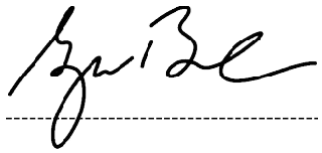
## Conclusion:

By following the steps outlined in this policy, SAFETY HOUSE aims to respond swiftly and effectively to any data breaches, protect affected individuals, and prevent future incidents. We are committed to complying with all relevant data protection legislation and upholding the highest standards of data security.

---

## Review of the Policy:

This policy will be reviewed annually by the **Data Protection Officer** to ensure its continued relevance and effectiveness. Updates to the policy will be communicated to all staff and relevant stakeholders.



CEO