Data Protection / GDPR Policy

| Version 1 – January 2023 |

Contents

Introduction

1. Purpose

The purpose of this policy and procedure is to ensure compliance of Staff Power Group with all of it's obligations as set out in the General Data Protection Regulation.

2. Data Controller

Staff Power Group is a Data Controller as defined in the General Data Protection Regulation 2018.

3. Notification with the Information Commissioner's Office (ICO)

Staff Power Group notified the ICO, when it was established, and have been registered for the duration the company has been trading.

Please follow the link for our registration details:

4. Definitions

- Personal data is information that relates to an identifiable living individual that is processed as data.
- Processing means collecting, using, disclosing, retaining, or disposing of information.
- The data protection principles apply to all information held electronically or in structured files that tells you something about an identifiable living individual.
- The principles also extend to all information in education records. Examples would be names of staff, learners, families, learners, subcontractors, dates of birth, addresses, national insurance numbers, school marks, medical information, SEN assessments and staff development reviews.
- Sensitive personal data is information that relates to race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexuality and criminal offences.
- There are greater legal restrictions on processing sensitive personal data than there are on personal data.

5. Data Protection Principles

The eight core principles of the Data Protection Act are enshrined in this policy and Staff Power Group commit that personal data:

- Is processed fairly and lawfully;
- Is obtained only for lawful purposes, and is not further used in any manner incompatible with those original purposes;
- Is accurate and, where necessary, kept up to date;
- Is adequate, relevant and not excessive in relation to the purposes for which it is processed;
- Is kept for longer than is necessary for those purposes;

- Is processed in accordance with the rights of data subjects under the DPA;
- Is protected by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage; and
- Is not transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection of the personal information.

6. Fair Processing

Staff Power Group is committed to being clear and transparent about what type of personal information we hold and how it is used.

The following 'Privacy Notice for staff, learners, guardians, learners and subcontractors' will be published on our website.

7. Privacy Notice

7.1 Why do we collect information?

Staff Power Group collects information and holds this personal data so that we can:

- Support each learners learning;
- Support each learner correctly
- Monitor and report progress of learners to funders;
- Monitor and evaluate outcome and measures
- Monitor progress
- Liaise with statutory services and legal services
- Provide appropriate support and
- Asses our effectiveness and competency.

7.2 What type of information do we collect?

The information will include:

- personal data such as name and date of birth as well as contact details and attendance information. It will also include sensitive personal data such as: ethnicity; special educational needs; incidents; and medical information that will help us to support each learner with wider welfare needs.
- We will also hold personal contact information about parents and carers, next of kin so that we can get hold of you/then routinely or in an emergency.
- CCTV is used in all communial areas at Hope Street Xchange, however we do not have access to this the University Campus Security does. This will only be for general security purposes in order to protect the building, staff and learners.
- Photographs and videos may be included, as part of your personal data and this will be treated with the same level of confidentiality as all other personal data. Photographic images used publicly which are available on media and web sites, newsletters will not identify learners unless permission has been given in advance. Nor will any images be used without prior consent.

7.3 Do we share this information with anyone else?

We do not share any of this data with any other organisation without your permission except where the law requires it. We are required to provide learner data to local and central government through the Department for Education (DfE www.education.gov.uk) and the Education Funding Agency (EFA www.education.gov.uk/efa). Where it is necessary to protect a learner, we will also share data with Crisis Team and/or the Police.

8. Information Security

8.1 Objective

The information security objective is to ensure that Staff Power Group ’s information base is protected against identified risks so that it may continue to deliver its services and obligations to the community. It also seeks to ensure that any security incidents have a minimal effect on its business and its operations.

8.2 Responsibilities

The Directors and management team of Staff Power Group have direct responsibility for maintaining the Information Security policy and for ensuring that the staff and volunteers adhere to it.

8.3 General Security

It is important that unauthorised people are not permitted access to Staff Power Group’s information and that we protect against theft of both equipment and information. This means that we must pay attention to protecting our buildings against unauthorised access. Staff must:

- Not reveal pin numbers or building entry passes to people that you do not know or who cannot prove themselves to be employees;
- Beware of people tailgating you into the building or through a security door;
- If you don’t know who someone is and they are not wearing some form of identification, ask them why they are in the building;
- Not position computer screens on desks where members of the public could see them;
- Lock secure areas when you are not in the office;
- Not let anyone remove equipment or records unless you are certain who they are;
- Visitors and contractors in Staff Power Group’s building should always sign in at the main reception.

8.4 Security of Paper Records

- Paper documents should always be filed with care in the correct files and placed in the correct place in the storage facility.
- Records that contain personal data, particularly if the information is sensitive should be locked away when not in use and should not be left open or on desks overnight or when you are not in the office;
- Always keep track of files and who has them;
- Do not leave files out where others may find them;
- Where a file contains confidential or sensitive information, do not give it to someone else to look after.
- Adhere to Staff Power Group’s clear desk policy

8.5 Security of Electronic Data

Most of our data and information is collected, processed, stored, analysed and reported electronically. It is essential that our systems, hardware, software and data files are kept secure from damage and unauthorised access.

Staff Power Group staff must:

- Prevent access to unauthorised people and to those who don't know how to use an item of software properly. It could result in loss of information;
- When we buy a license for software, it usually only covers a certain number of machines. Make sure that you do not exceed this number, as you will be breaking the terms of the contract.
- Passwords are a critical element of electronic information security. All staff must manage their passwords in a responsible fashion:
    - Don't write it down;
    - Don't give anyone your password;
    - Your password should be at least 6 characters;
    - The essential rules your password is something that you can remember but not anything obvious (such as password) or anything that people could guess easily such as your name;
    - You can be held responsible for any malicious acts by anyone to whom you have given your password;
    - Include numbers as well as uppercase letters in the password;
    - Take care that no-one can see you type in your password;
    - Change your password when prompted. Also change it if you think that someone may know what it is.
    - Many database systems, particularly those containing personal data such as our Management Information System should only allow a level of access appropriate to each staff member. The level may change over time.

8.6 Use of E-Mail and Internet

- The use of Staff Power Group's e-mail system and wider Internet use is for the professional work of Staff Power Group. Reasonable personal use of the system in a member of staff's own time is permitted but professional standards of conduct and compliance with Staff Power Group's wider policies are a requirement whenever the e-mail or Internet system is being used. Staff Power Group access via Sunderland University uses a filtered and monitored broadband service to protect people's data. Deliberate attempts to access web sites that contain unlawful, pornographic, offensive or gambling content are strictly prohibited. Staff discovering such sites on the system must report this to Staff Power Group Directors immediately.
- To avoid a computer virus, malware or ransomware arriving over the Internet, do not open any attachments which you are either not expecting or from an unknown sender.
- Do not send highly confidential or sensitive personal information via e-mail unless password protected, otherwise it must be hand delivered or collected and signed for;
- Save important e-mails straight away;
- Unimportant e-mails should be deleted straight away;
- Do not write anything in an e-mail which could be considered inaccurate or offensive, and cannot be substantiated.

8.7 Electronic Hardware

- All hardware held within Staff Power Group should be included on the asset register;
- When an item is replaced, the register should be updated with the new equipment removed or replaced;
- Do not let anyone remove equipment unless you are sure that they are authorised to do so;

8.8 Homeworking Guidance

If staff must work outside of Staff Power Group or at home, all of the 'Information Security' policy principles still apply. However, working outside of Staff Power Group presents increased risks for securing information.

The following additional requirements apply:

- Do not access confidential information when you are in a public place, such as a train and may be overlooked;
- Do not have conversations about personal or confidential information on your mobile when in a public place. Ensure that, if urgent, you have your conversation in a separate room or away from other people;
- The Dropbox account should be used so confidential documents do not have to be taken off site whenever possible so data is still being held securely on Staff Power Group's servers.

If you use a laptop, tablet or smart phone:

- Ensure that it is locked and password protected to prevent unauthorised access;
- Make sure that you don't leave your device anywhere it could be stolen.
- Keep it with you at all times and secure it when you are in Staff Power Group's premises
- Portable devices or memory sticks that contain personal data must be encrypted. Taking personal data off-site on a device or media that is not encrypted is a disciplinary matter;
- Ensure personal data is not stored on the hard drive of a personal device;
- When working on confidential documents at home do not leave them lying around where others may see them; dispose of documents using a shredder;
- If you are using your own computer, ensure that you access and work from Staff Power Group's Dropbox.
- Do not transfer documents and data to your own machine.
- **It is forbidden to use a computer owned by you to hold personal data about learners or staff** at Staff Power Group .

8.9 Audit of Data Access

Where possible our software specifications will include the function to audit access to confidential data and attribute access, including breaches of security, to specific users.

8.10 Data Backup

- Staff Power Group will arrange that all critical and personal data is backed up to physical storage.
- Data backup should routinely be managed on a rolling daily process to secure off-site areas.
- An offsite backup of key financial and MIS data is scheduled each night.

9. Disposal of Information

- Paper records should be disposed of with care.
- If papers contain confidential or sensitive information they must be placed in the confidential bins for secure collection or shredded before disposing of them.
- Particular care must be taken when selecting papers to be placed in a recycling bin.
- Computers and hardware to be disposed of must be completely 'cleaned' before disposal.
- It is not enough just to delete all the files.
- It cannot be assumed that simply deleting a file will prevent it being recovered from electronic media. Electronic memory containing personal information or sensitive personal information must be electronically scrubbed or physically destroyed.
- Where a third-party contractor holds personal information on behalf of Staff Power Group, for example a software provider, accountants; Staff Power Group will seek reassurance from the contractor regarding their data protection policies and procedures.

10. Subject Access Requests

- Any requests for access to personal data or educational records will be dealt with as described in the Privacy Notice;
- Staff Power Group staff may have access to their personal data within 30 calendar days of a request and at no charge.
- Staff Power Group will maintain a documented record of all requests for personal information with details of who dealt with the request, what information was provided and when, and any outcomes. The record will be used if there is a subsequent complaint in relation to the request.

11. Sharing Personal Information

- Staff Power Group only shares personal information with other organisations where there is a legal requirement to do so or the organisation has been contracted by Staff Power Group to carry out a function of Staff Power Group.
- Staff Power Group is required, for example, to share information with the Department for Education and the Education Funding Agency.
- The Director will be responsible for authorising the sharing of data with another organisation. The principle, in authorising the sharing of data will take account of:
    - Whether it is lawful to share it;
    - Whether there is adequate security in place to protect the information while it is being transferred and then held by the other organisation;
    - Include in the Privacy Notice a simple explanation of who the information is being shared with and why.

Considerations regarding the method of transferring data should include:

- If personal data is sent by e-mail then security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending the message. The data may also need to be password protected and the password sent separately. You should also check that it is going to the correct e-mail address.
- Circular e-mails sent to learners should be sent bcc (blind carbon copy) so that the e-mail addresses are not disclosed to everyone.
- Similar considerations apply to the use of fax machines. Ensure that the recipient will be present to collect a fax when it is sent and that it will not be left unattended on their equipment.
- If confidential personal data is provided by paper copy it is equally important to ensure that it reaches the intended recipient.

12. Websites

- Staff Power Group's website will be used to provide important information including our Privacy Notice.
- Where personal information, including images, are placed on the web site the following principles will apply:
    - We will not disclose personal information (including photos) on a web site without the appropriate consent;
    - Comply with regulations regarding cookies and consent for their use;
    - Our website design specifications will take account of the principles of data protection.

13. Photographs and Videos

- Staff Power Group will use, to show inclusion and promote the work we are doing, on websites, social media and publications without further specific consent being sought after initial consent is given, unless you withdraw your consent.
- All other uses by Staff Power Group of photographic images and videos are subject to data protection.
- These images if used in publications and website will be shared for the purpose stated in consent.

14. Processing by Others

Staff Power Group remains responsible for the protection of data that is processed by another organisation on its behalf. As part of a contract of engagement other organisations that process data on behalf of Staff Power Group will have to specify how they will ensure compliance with data protection law.

15. Training

The Director and line managers will ensure that all staff are adequately trained to understand their responsibilities in relation to this policy and procedures.

16. Policy Review

Policy Commencement Date	4th January 2021
Policy Version	Version 1.0
Date of Review	January 2023
Date of next review	January 2024
Signature	L. Johnston