General Data Protection Regulations Policy

PURPOSE: To inform staff, students, and visitors of the AccXel Policy and how to request access to data.

SCOPE: This policy applies to all AccXel staff, contractors, and learners.

RESPONSIBILITY: The AccXel Senior Management team ('SMT') is responsible for this Policy.

General Data Protection Regulations Statement of Intent:

1. This policy applies to all employees (permanent and temporary), learners and other users of AccXel Company Data.

2. The Company holds personal and confidential data about its employees, students, employee applicants, board members and tenants. All individuals have a right to privacy under the Data Protection Act 2018.

3. This policy sets out how the Company protects and promotes the rights of individuals and groups. It identifies the information that is to be treated as confidential and the procedures for collecting, storing, handling, and disclosing such information.

4. This policy will ensure that the Company complies with the fair processing code regarding the collection and use of the data collected.

5. This policy will ensure that all persons processing personal data on behalf of the Company receive adequate and periodical awareness training to ensure that they understand their

contractual and legal responsibility towards the personal information processes in their day-to-day work.

General Data Protection Regulations Policy:

1. **Introduction:**

AccXel needs to keep certain information about its employees, students, and other users to enable, for example, the monitoring of performance, achievements, and health and safety. It is also necessary to process information so that the Company can recruit and pay staff, organise courses and comply with legal obligations to funding bodies and government. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the Company must comply with the GDPR Principles which are set out in the Data Protection Act 2018 (the 2018 Act). In summary, the Act requires personal data to be:

- Obtained and processed fairly and lawfully and not to be processed unless certain conditions are met.
- Obtained for a specified and lawful purpose and not to be processed in any manner incompatible with that purpose.
- Adequate, relevant, and not excessive for those purposes.
- Accurate and kept up to date.
- Kept for no longer than is necessary for that purpose.
- Processed in accordance with the data subject's rights.
- Kept safe from unauthorised access, accidental loss, or destruction.
- Transferred to a country outside the European Economic Area only if that country has equivalent levels of protection for personal data.

The Staff Guidelines for Data Protection (see Appendix 1) detail the impact and responsibility of staff and students in relation to each of the eight Data protection Principles.

All staff and others who process or use any personal information must ensure that they always follow these principles. This Data Protection Policy has been drawn up to help in securing compliance with the legislation.

2. **Status of the Policy:**

- This policy is a condition of employment. Staff must abide by the rules and policies made by the Company from time to time. Any failures to follow the policy may therefore result in disciplinary proceedings.

- Any member of staff who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the designated Data Protection Officer initially. If the matter is not resolved, it may be raised through the grievance procedure.

3. **The Data Controller:**

- The Data Protection Officer for the Company is the AccXel Managing Director, Nicola Bird.

4. **Notification of data held and processed:**

All staff, learners and other users are entitled to know:

- What information the Company holds about them and processes and why.
- How to gain access to the information (see paragraph 8).
- How to keep it up to date.
- What the Company is doing to comply with its obligations under the 2018 Act.

5. **Responsibilities of staff:**

All staff are responsible for:

- Checking the information that the Company sends out from time to time which gives details of information kept and processed about staff.
- Checking that any information that they provide to the Company in connection with their employment is accurate and up to date.
- Informing the Company of any changes to the information which they have provided (eg changes of address);
- Informing the Company of any errors or changes (the Company cannot be held responsible for errors if the member of staff has not brought them to the Company's attention).

If and when, as part of their responsibilities, staff collect information about staff, students or other people, (e.g. about students' course work, opinions about staff / students ability, references to other institutions or companies, or details of personal circumstances), they must comply with the guidelines for staff in Appendix 1.

The data collected on approved forms and any data must not be used to develop localised data collection and reporting systems.

6. Data security:

All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely.
- Personal information is not disclosed either orally or in writing or accidentally or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter and may be regarded as gross misconduct in some cases.

Personal information should be:

- Kept in a locked filing cabinet, or in a locked drawer.
- If it is computerised, be password protected or kept only on disk which is itself kept securely.

All staff should ensure that they comply with any subject consent requirements as set out in paragraph 11.

All staff should ensure that they do not take electronic personal data off company premises. When transferring and sharing data with external organisations, such as the funding bodies or Auditors, necessary security arrangements will be adhered to using encryption and following appropriate protocols agreed by the Data Protection Officer.

7. Learner's obligations:

Learners must ensure that all personal data provided by the Company is accurate and up to date. They must ensure that changes of address, etc are notified in writing using the appropriate change of details form to their tutor.

Students who use Company computer facilities may, from time to time, process personal data. If they do, they must notify their tutor. Any student who requires further clarification about this should contact the head of Education.

Tutors will make students aware of their responsibilities under this section as part of the student induction to their course.

8. Rights to gain access to information:

Staff, students, and others have the right to gain access to any personal data that is being kept about them either on computer or in certain files. The Company will provide on request to all staff, students, and other users a standard form of notification. This will show all the types of data the Company holds about them and processes, and the reasons for which it is processed. Any person who wishes to exercise this right should send a written request to the operations director. To gain access, an individual may wish to receive notification of the information currently being held. This request should be made in writing using the standard form attached (Appendix 2).

The Company aims to comply with requests for access to personal information as quickly as possible and within the statutory deadline of 40 days.

9. Publication of Company information

Information that is already in the public domain is exempt from the 2018 Act. It is the Company's policy to make public information. The following information will be available to the public for inspection:

- Names of Company owners
- Names of staff (with consent)
- Photographs of key staff and governors
- Registers of interests
- Information shown in the policy statement on access to information (if containing personal information, then consent may be required)

Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the designated Deputy Data Protection Officer. The Company's internal phone and e-mail address lists will not be public documents.

10. Subject consent:

In many cases, the Company may process personal data only with the written consent of the individual. In some cases, if the data is sensitive, express written consent must be obtained. Agreement to the Company processing some specified classes of personal data is a condition of acceptance of a student onto any course and a condition of employment for staff. This includes information about previous criminal convictions.

Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 16 and 18. The Company has a duty under the Children Act and other enactments to ensure that staff are suitable for the job, and students are suitable for the courses offered. The Company has a duty of care to all staff and students and will take such steps as may be reasonably practicable to make sure that employees and those who use the Company facilities do not pose a threat or danger to other users.

The Company will also ask for information about health needs, such as allergies and forms of medication, or any conditions such as asthma or diabetes. The Company will only use the information in the protection of the health and safety of the individual but will need written consent to process it in the event, for example, of a medical emergency.

All prospective staff and students will be asked to sign a Consent to Process form, relating to types of information, when an offer of employment or a course place is made. A refusal to sign such a form may result in the offer being withdrawn.

11. Processing Sensitive Information and Data Subject Information Requests:

Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This may be necessary to ensure the Company is a safe place for everyone, or to operate other Company policies, such as the sick pay policy or equal opportunities policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will be asked to give express consent for the Company to do this. Offers of employment or places on courses may be withdrawn if an individual refuses to consent to this without good reason.

The Managing Director should be consulted when requests for information about students are received from the police, statutory bodies, solicitors and third parties. All disclosures must be made with consent or in accordance with a non-disclosure exemption as provided in the Act, such as Crime and Taxation which would cover disclosures to the Police providing requirements of the exemption are complied with.

12. Examination marks:

Students will be entitled to information about their marks for both coursework and examinations.

13. Retention of data:

Data will be retained in accordance with the law. Unless stated by specific awarding bodies course work and portfolio data will be kept for five years. Hard copy will be securely shredded electronic data will be deleted. Student work and portfolios will be offered back to the student.

14. Transferring of personal or sensitive data via e-mail:

Users should not use the services of the Company Internet and / or e-mail to obtain or send material which contravenes the law or published Company policies.

Users are advised that the use of e-mail to send personal data to a third party is expressly forbidden unless prior approval is obtained from the Company's Data Protection Officer.

Users are advised that all e-mails sent from an account is the responsibility of the individual account holder.

15. Transferring of personal or sensitive data outside of the EEA:

Personal data must not be transferred to a country outside the EEA unless that country has equivalent levels of protection for personal data. Therefore, any personal data being sent outside of the EEA must be approved by the Data Protection Officer. This includes all electronic forms of communication, such as personal information being posted on the Company's website or held on "the Cloud".

16. Conclusion:

Compliance with the 2018 Act is the responsibility of all members of the Company. Any deliberate breach of the Data Protection policy may lead to disciplinary action being taken, or access to Company facilities being withdrawn, or even to a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Officer or designated Deputy Data Protection Officer.

Note that from September 2020 it is a requirement under ESFA funding rules that AccXel holds a Cyber Security certificate and from September 2021 a Cyber Essentials Plus certificate.

Appendix 1

Staff Guidelines for compliance with General Data Protection Regulations (In accordance with the eight Data Protection principles set out in the Data Protection Act 2018 and referred to in paragraph 1 of this Policy).

1. All staff will regularly process data about students, when completing registers, marking course work, writing reports or references, or as part of a pastoral or academic supervisory role. The Company will ensure, through admission and registration procedures, that all students give their consent to this sort of processing, and are notified of the categories of processing, as required by the 2018 Act. The information with which staff deal on a day-to-day basis will be 'standard' and will cover categories such as:

- General personal details such as name and address.
- Details of class attendance, course work marks and grades and associated comments.
- Notes of personal supervision, including matters about behaviour and discipline.

2. Information about a student's physical or mental health; sexual life; political or religious views; trade union membership; and ethnicity or race is sensitive and can only be collected and processed with the student's express consent. If staff need to record this information, they should use the Company standard form (eg: for recording information about dietary needs, for religious or health reasons prior to taking students on a field trip; recording information that a student is pregnant, as part of pastoral duties).

3. All staff have a duty to make sure that they comply with the data protection principles which are set out in the Company Data Protection Policy. All staff may at some stage during their employment with the Company encounter, and process personal and possibly sensitive personal data. It is essential that staff are aware of their responsibilities under the Act and process any such data in accordance with the Company Data Protection Policy. Staff must ensure that records are:

- Accurate.
- Up to date.
- Fair.

- Kept and disposed of safely, and in accordance with Company policy.

4. Staff must not disclose personal data to any student, unless for normal academic or pastoral purposes, without authorisation or agreement from the data controller, or in line with Company Policy.

5. Staff must not disclose personal data to any other member of staff except with the authorisation, or in line with Company policy.

6. Before processing any personal data, all staff should consider the following checklist:

- Do you really need to record the information?
- Is the information 'standard' or is it 'sensitive'?
- If it is sensitive, do you have the data subject's express consent?
- Has the student or member of staff been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the data subject's consent to process the information, are you satisfied that it is in the best interests of the student or the staff member to collect and retain the data?

Appendix 2

Standard Request Form for Access to Data

I (print name) ……..

Address / Contact Details: ……..

……

Wish to have access to: Either (delete as appropriate):

a) All the data that the Company currently has about me, either as part of an automated system or part of a relevant filing system.
or:
b) Data that the Company has about me in the following categories:

- Academic marks or course work details
- Academic or employment references
- Disciplinary records
- Health and medical matters
- Trade union information (including political)
- Any statements of opinion about my abilities or performance
- Personal details including name, address, date of birth etc

Please tick the appropriate box(es)

I am currently either (please delete as appropriate):

a employed at AccXel or

b enrolled as a student AccXel

Signed: ……

Date: ……..

Please submit completed form to the Training operations Director

This request will not be processed unless this form is signed. The company may request confirmation of ID in certain circumstances.

This policy has been agreed by the AccXel senior management team and agreed. It will be reviewed every two years or after significant changes to the centre’s business or staff.

Signed:  Date: 06/01/2024