Family:	Leadership and Management	REF: ARCPO008
Policy title	GDPR Policy	
Version:	3.4	
Policy owner:	Operations Director	
Policy author:	Quality Manager	
Date of Review	2/1/2024	
Next review date	02/1/2025 (Annual Review)	
Applies to:	All staff	
Related policies:	Learner Handbook Staff Handbook Staff Selection and Recruitment Process Staff CPD Policy IQA Handbook Complaints and Praise Policy	

Policy Introduction

ARC is committed to a policy of protecting the rights and privacy of individuals, including learners, staff and others, in accordance with the General Data Protection Regulation (GDPR) May 2018. ARC Group is not only committed to legal compliance, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all Personal Data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

This policy sets out the procedures that are followed when dealing with personal data. The regulation defines “Personal Data “as any information relating to an identified or identifiable natural person (a “data subject”); an identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural, or social identify of that natural person.

Policy Aim

ARC needs to process certain information about its staff, learners, customers and other individuals with whom it has a relationship for various purposes such as, but not limited to:

- The recruitment and payment of staff.
- The administration of courses.
- Learner enrolment.
- Examinations and external accreditation.
- Recording learner progress, attendance and conduct.
- Collecting fees.
- Complying with legal obligations to funding bodies and government including local government.

To comply with various legal obligations, including the obligations imposed on it by the General Data Protection Regulation (GDPR) ARC must ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

To ensure that this happens, ARC Group has developed the Data Protection Policy and is registered for Notification under the Act.

The Group holds information about its members, employees, learners, partners, suppliers and other users as a normal part of its day-to-day business. The Group will ensure that the interests of its employees and learners are safeguarded by regularly reviewing its policy (annually) and taking account of Codes of Practice and other advice issued by the Information Commissioner. It will also take account of the wider legal framework and their impact in respect of Data Protection. The Group acknowledges that the Corporation or individual members of staff may be held liable for criminal offences under the Data Protection Act 1998. Fines for breaches are unlimited.

Interpretation of the Data Protection Act 2018

The Data Protection Act 2018 places duties and obligations on "Data Controllers" in relation to their "processing" of "personal data". Personal data includes information about living, identifiable individuals (data subjects) that is to be processed by means of automated equipment (including computer processing and CCTV images). This may include e-mails which are processed with reference to the data subject. Personal data also includes information recorded as part of a "relevant filing system". This is any manual filing system, microfiche or paper set of information that is structured in such a way that information relating to a particular individual is readily accessible.

Personal data must be processed fairly and lawfully. There must be a clear purpose for processing. Processing means obtaining, recording, holding or carrying out any operation on the information or data.

Sensitive personal data is a special category. It may only be processed with the explicit consent of the data subjects:

- the racial or ethnic origin of the data subject;
- political opinions;
- religious or other beliefs of a similar nature;
- trade union membership;
- physical or mental health or condition;
- sexual life;
- the commission or alleged commission of any offence;
- proceedings for any offence or alleged offence.

Core Data Protection Principles state that personal data must be: -

1. fairly and lawfully processed;
2. processed for limited purposes;
3. adequate, relevant and not excessive;
4. accurate;
5. not kept for longer than is necessary;
6. processed in accordance with individuals' rights;
7. secure;
8. not transferred to countries without adequate protection.

Rights for Individuals under the Data Protection Act

- right of subject access (to data held on computer records and relevant filing systems upon making a request in writing and paying a fee);
- right to prevent processing likely to cause unwarranted and substantial damage or distress;
- right to prevent processing for the purposes of direct marketing;
- right to compensation;
- right to correction, blocking, erasure or destruction;

- right to ask the Information Commissioner to assess whether the Data Protection Act has been contravened.

Criminal Offences under the Data Protection Act

- processing without notification.
- failure to comply with an enforcement notice.
- unlawful obtaining or disclosure of personal data.
- selling or offering to sell personal data without the consent of the data subject.

Group Procedure

The Group, as a corporate body, is the Data Controller under the Act and the Corporation is therefore ultimately responsible for implementation.

The designated Data Controllers on behalf of the Group are:

- Managing Director
- Operations Director
- Performance Manager
- HR Manager

The Data Controllers are responsible for data within their normal line management responsibility within the Group. The Quality Manager will be responsible for convening a Data Protection team. The Data Protection Team will be responsible for:

- Data Protection Policy.
- The Data Protection Notification.
- Review of procedures.
- Data Protection audits.

Responsibilities of Staff

The Group will require all staff to familiarise themselves and comply with the GDPR Policy.

Responsibilities of Learners

The Group will require all students to consent to processing under the GDPR Policy.

Responsibilities of Partners

A Data Protection Memorandum of Understanding will be included in all contracts where third parties process data on behalf of the Group and where third parties have access to data as a necessary part of their contracted work.

Notification of Data Held and Processed

All staff, learners and other users are entitled to:

- Know what information the Group processes about them and why
- Know how to gain access to it
- Know how to keep it up to date
- Know what the Group is doing to comply with its obligations

Conditions for Processing

Authorised processing of information takes place as part of the day-to-day business of the Group in accordance with the schedule in the Group's Data Protection Act Notification.

Conditions for authorised processing may include:-

- consent of the data subject
- necessary for the legitimate interests of the Group or by third parties to whom the data is disclosed except where processing is unwarranted because of prejudice to legitimate interests of the data subjects
- necessary for a contract with the data subject
- necessary to protect the vital interests of the data subject
- necessary for the administration of justice
- necessary for any enactment
- necessary function of a Crown Minister, or government department necessary functions of a public nature exercised in the public interest

Subject Access Rights to Information

Learners and other users of the Group have subject access rights to certain personal data that is being held about them either on computer or in manual files. Any person who wishes to exercise this right should put their request in writing.

Subject access requests for staff should be made in writing to the HR Manger.
Subject access requests for learners should be made in writing to the Operations Director.

Any other requests should be made in writing to the Operations Director. The data subject must supply sufficient information to enable the Group to locate the information that the subject seeks. The Group is not obliged to comply with open ended requests. The Group may refuse to disclose data that makes reference to the personal data of third parties. The Group aims to comply with requests for access to personal information as quickly as possible and will ensure that it is provided within 40 calendar days unless there is good reason for the delay. In such cases, the reason for delay will be explained in writing to the data subjects making the request at the earliest possible opportunity.

Disclosure of Personal Data

Disclosure of data to authorised recipients takes place as part of the day-to-day business of the Group. Authorised disclosure will take place according to the schedule in the Data Protection Act Notification.

Personal data must not be disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Particular discretion must be used before deciding to transmit personal data by fax or email. Where non-routine requests are made, or where staff are unsure of their responsibilities, they should seek the advice of their line manager. The line manager may decide to refer a request for a definitive decision to the Operations Director who is the Data Manager. The Data Manager will provide advice about the interpretation of the Act.

Staff should be aware that those seeking information about individuals may use deception to obtain information. Staff should take steps to verify the identity of those seeking information, for example by obtaining the telephone number and returning the call or by reviewing identification documents if an application is made in person.

All applications for data should be made in writing and e-mail requests will be accepted. Request by other public bodies, including the police, must meet the requirements for lawful processing. The police must be able to demonstrate that they require the information in pursuit of a criminal investigation. Where a disclosure

is requested in an emergency, staff should make a careful decision as to whether to disclose, taking into account the nature of the information being requested and the likely impact on the subject of not providing it.

Disclosure of Data to Employers

Many learners attend courses under the sponsorship of their employers. This may include paid time to attend or payment of fees. These learners will be required to consent to the sending of routine reports to their employers on academic progress and attendance as part of their "Data Protection Consent to Process" on the enrolment form.

Subject Consent

In many cases, the Group can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent, must be obtained. Agreement to the Group processing some specified classes of personal data is a condition of acceptance of a learner onto any course, and a condition of employment for staff.

Some jobs or courses will bring the applicants into contact with young people and vulnerable adults. The Group has a duty to ensure staff are suitable for the job, and learners for the courses offered. The Group also has a duty of care to all staff and learners and must therefore make sure employees and those who use the Group's facilities do not pose a threat or danger to other users. Where appropriate therefore the College will obtain information about previous criminal convictions. The Group will notify all users at the point where information is collected from them which information will be processed and the purpose of processing under the Data Protection Act. The consent of the user will be obtained at the point of collection.

This includes;

- Application forms for staff
- Enrolment forms
- Telephone enquiries and applications
- Internet enquiries/e-mail, applications and enrolments

The Group will also ask users to consent to receive promotional campaign details about additional activities and further study opportunities that may be of interest to them. Users have a right to decline receipt of this information.

The Group will ask learners to consent to disclosure of information to employers, where learners are sponsored by employers to attend college.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender or family details. This may be to ensure the Group is a safe place for everyone, or to operate other Group policies. 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 learners will be asked to give express consent for the Group to do this.

Publication of Group Information

Information that is already in the public domain is exempt from the Act. It is ARC Group policy to make as much information public as possible. Types of information available are recorded in the Group's Publication Scheme in compliance with the Freedom of Information Act 2000.

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 know that unauthorised disclosure may be regarded as a disciplinary matter. Personal information should be:

- Secured in a locked filing cabinet or desk drawer.
- If it is computerised, be password protected.

Particular care must be taken with data held on portable disks or laptop computers. Staff should ensure that casual disclosure does not take place; by, for example, leaving computer printouts uncovered on desktops or by allowing unauthorised users to view computer screens. Computer printouts must be kept securely and destroyed in a confidential manner.

Offices where staff are employed to process personal data should be locked when not occupied. Staff should take particular care with data that has been processed while working at home. All staff and students are responsible for ensuring that they observe the procedures of other appropriate Group policies.

Retention of Data

Personal data will be retained for no longer than is necessary for the purpose for which it was collected. Standard retention times are necessary to meet various contractual requirements. Standard retention times for related documents are specified in the Financial Regulations.

Disposal of Data

Particular care must be taken with the disposal of personal data. Staff should be aware that the same standards should be applied to informal records, lists and printouts held by individual members of staff containing personal data as to records which are part of the formal records system. Personal data must be destroyed by secure methods such as shredding or confidential waste sacks handled by authorised contractors. Formal records may only be destroyed with the appropriate authority

Examination Results/News

Learners will be entitled to information about their marks for both coursework and examinations. The Group may withhold certificates, accreditation or references if the full course fees have not been paid or equipment have failed to be returned.

News stories focussing on individual students will only be made available with the consent of the learner.

References

The provision of a reference will generally involve the disclosure of personal data. The Group is responsible for references given in a corporate capacity. The Group will not provide subject access rights to confidential references written on behalf of the Group about employees and students and sent to other organisations. This is a specific exemption allowed by the Act. The Group recognises that once the reference is with the organisation to whom it was sent then no specific exemption from subject right access exists. The Group will

normally provide subject right access to confidential references received about employees and learners provided to the Group by other organisations. However, the Group may withhold information under the auspices of the Act; as deemed appropriate.

Direct Marketing

The Group will only use personal data for promotional campaigns or to market additional activities to existing or previous learners where they have given consent.

Complaint handling

Data subjects with a complaint about the processing of their personal data, should put forward the matter in writing to the Operations Director. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Operations Director will inform that data subject of the progress and outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation between the data subject and the Operations Director then the data subject may, at their option, seek redress through a formal complaint to the data protection authority within the applicable jurisdiction.

Breach reporting

Any individual who suspects that personal data breach has occurred due to the theft or exposure of personal data must immediately notify Data protection officer providing a description of what occurred. Notification of the incident can be made via:
Email:gareth.jones@thearcgroup.co.uk
Phone: 01443693431
Writing: Unit 4 and 5 Centre court, Treforest industrial estate, Pontypridd, CF37 5YR

Signed: 

Chris Davis

Date: 2/1/2024

Managing Director

Signed: 

Gareth Jones

Date: 2/1/2024

Operations Director

Appendix for Medical specific GDPR Protection

Policy Aim

ARC Medical needs to process certain information about its staff, customers, and other individuals with whom it has a relationship for various purposes such as, but not limited to:

- The administration of medical screening, drug & alcohol testing
- Recording customer screening results

Purposes for which Personal Data may be held

Personal data relating to employees may be collected primarily for the purposes of:

- Chain of custody form – including all personal data
- Medical evaluation
- Results of medical assessment and drug & alcohol screening pass or fail

Sensitive personal Data

Sensitive personal data includes information relating to the following matters:

- His/her/their physical or mental health or condition
- Results of medical assessment
- Results of drug & alcohol screening

To hold sensitive personal data ARC Medical must additionally satisfy a sensitive data condition. The most appropriate condition for medical accreditation purposes is that the processing is necessary to enable ARC Medical to meet its legal obligations (for example, to ensure health and safety or to avoid unlawful discrimination).

Responsibility for the processing of personal data

The only employees who have access to any information in the ARC Medical are the Department manager, Booking Coordinator, Health Assessment Nurse, Collection Officer, and responsible Occupational Health Physician.

Access to personal data ('Subject Access Requests')

The responsible occupational physician will review the individuals' data before it is revealed to remove any data that could be detrimental to the individual or contains information regarding another person.

Storage of records

All records of individuals who have undertaken medical assessment/screening will be held for a minimum of 10 years, if a 'fail' result is obtained these records must be held for no less than 40 years, but in accordance with NR/L2/OHS/00120 should be retained indefinitely by the employer and medical provider.

All current hard copy records are stored in a locked, fireproof cabinet and only accessed by authorised personnel (Department Manager, Medical Booking Coordinator, Health Assessment Nurses, Collection Officers, Directors and named responsible health physician. These records are all stored electronically on a password-controlled OneDrive cloud. After each RISQS audit the previous 12 months hard copy records are shredded and only an electronic copy is maintained for the period of time detailed above.

Communication of Information

Email: *a named responsible person must be allocated from each company to which the screening results are sent, the email address must be confirmed. The email must be marked confidential.*

Telephone: *a named responsible person must be allocated from each company to which screening results are communicated. When donors are being contacted with their results it must be through their provided telephone details on the medical questionnaire, the results may only be provided to the donor, no other person who answers the provided telephone number can be informed of the results. Telephone calls to companies/donors must be conducted in a confidential manner, where no one else can overhear the information (only the person making the call is present in the room at the time of the call and the door is shut).*

Transfer of documents upon change of contract and close of business

If, at such time as ARC Medicals ceases trading and the department is bought out by another company, ARC will request a nominated person to whom the documents will be transferred to, upon production of a valid ID and confirmation that they are responsible under the new company for the records. This transfer will take place face to face with the Data Controller of ARC and the nominated person as detailed above. A formal procedure will be agreed and signed; a copy retained by both parties. ARC will also produce a formal document listing all the documents to be transferred. ARC has a duty to inform all individuals that we hold data on, of the transfer of their documents. If there is a change of contract the client is responsible for informing their employees of the change.