The Rural Enterprise Academy

General Data Protection Regulation (GDPR) Policy

Approved by Governors: **March 2018**
Review Period: **2 years**
Review by: **March 2020**

General Data Protection Regulation (GDPR) Policy

1.0 Policy Statement

1.1 The General Data Protection Regulation (GDPR) replaces the Data Protection Act 1998 (DPA) which came into force on 1st March 2000 in the UK. It governs the processing of personal data and becomes legally enforceable in the UK on 25th May 2018, although the legislation is already legally approved.

This evolution of data protection regulation law was introduced to extend the protection of 'personal data' and clearly defines regulations on who can decide how and why personal data is processed with clear obligations to ensure that appropriate procedures and processes are in place to enable good information management, as defined by a set of clear principles and rules.

For the purposes of the GDPR personal data is defined as *"any information relating to an identified or identifiable natural person".*

The key principles of the new GDPR are:-

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

The Academy holds personal data about employees, learners, suppliers and wider individual data for a variety of purposes necessary to conduct its business.

This policy sets out how we will protect personal data and ensure that all staff understand the rules and principles governing the use of personal data which they may access in undertaking their duties. It is a requirement of this policy that staff must ensure that the Data Protection Officer (DPO) is consulted before any significant new data processing activity is initiated to ensure compliance with the relevant regulations and legislation.

This policy does not form part of the formal contract of employment but it is a condition of employment that employees will abide by the rules and regulations it outlines. Any failure to comply with the policy could therefore result in disciplinary proceedings.

All staff are responsible for:-

- Checking that any information provided to the College and the Academy in connection with employment is accurate and up-to-date.

- Informing the College and the Academy of any changes to information they have provided such as change of address.

- The College and the Academy cannot be held accountable for any errors unless staff have informed the College and the Academy of them.

2. Scope

2.1 The General Data Protection Regulation (GDPR) applies equally to digital and/or paper records held in any system from which any individual might reasonably be identified.

As with existing data protection legislation the GDPR can apply to personal data held visually in photographs or video clips (including CCTV) or as sound recordings. The Academy collects a large amount of personal data every year and has a responsibility to ensure full compliance with the letter and spirit of both current data protection legislation and the extended rights and responsibilities of the GDPR.

3. Key Principles

3.1 Awareness

It is the responsibility of all staff, including Governors of the Academy, to ensure adequate awareness of their responsibilities under the GDPR and wider data protection legislation. This should be appropriately referenced within the Academy 'Risk Register'.

3.2 Information Audit

The Academy must document the information it holds, the source and location of the data and who is responsible for it. Additionally the requirements of the GDPR place a greater emphasis on the maintenance and accuracy of data held, especially if that data is processed with an external agency. Any changes to the data that fall into this context must be passed onto wider agencies involved.

3.3 Privacy Information

The Academy must review its privacy notices and ensure that appropriate plans and processes are in place to comply with the letter and spirit of the GDPR.

The Academy must make the legal basis for collection of data transparent, document data retention periods and inform people that they have a right to complain to the ICO (Information Commissioner's Office) if they perceive a problem with the processing of the data warrants it.

3.4 Individual rights

The Academy must ensure systems and processes are in place to support the relevant rights of individuals in regard to their personal data including the deletion of

personal data where appropriate and how data will be made available electronically or in a commonly used format as required.

The GDPR protects the following specific data rights for individuals:

- The right to be informed
- The right of access
- The right of rectification
- The right to be forgotten (erasure of data)
- The right to restrict processing of data in specific circumstances
- The right to data portability
- The right to object to the use of personal data
- The right not to be subject to automated data driven decision making processes such as analytics profiling and auto-completion of opt-in on forms or similar.

3.5 **Subject Access Requests**

In most cases the Academy will not be able to charge for any requests made.

The Academy will have a total of one month to comply with a subject access request. Currently the law permits 40 days.

The Academy can charge for any request that is considered to be unfounded or excessive in regards to resource implications.

If the Academy refuses a request the Data Protection Officer must justify to the individual why the request has been refused and clarify that they have the right to complain to the supervisory authority to seek judicial remedy. This must be actioned quickly and within a maximum of one month.

3.6 **Lawful Basis for Processing Data**

For The Rural Enterprise Academy the lawful basis for the processing data in regard to the GDPR is the Education Act 1996. This is referenced on key forms and places relevant to data capture and processing.

3.7 **Consent**

Consent to process personal data must be based on the following principles. The consent must be freely given, specific, informed and unambiguous.

Affirmative action must be taken to opt in to any data processing where relevant.

There is no requirement to re-work all existing consent processes but compliance with the GDPR must be achieved.

3.8 **Children**

The GDPR for the first time provides special protection for the personal data of children.

The GDPR defines the age of a child in regard to consent for data processing as anyone under the age of 16. It is possible that for the UK this may be lowered to 13 but currently the legislation states 16. For anyone below this age, consent must be secured from a person with 'parental responsibility' for the purposes of data processing.

3.9 **Data Breaches**

The Academy must ensure it has appropriate procedures in place to detect, report and investigate a personal data breach. The data breach process is provided in Appendix 1 to this policy.

The Academy is only obligated to report a data breach to the ICO where it is likely to result in a risk to the rights and freedom of individuals, for example where it might lead to reputational damage, loss of confidentiality, discrimination or wider social or economic disadvantage.

If a member of staff becomes aware of a possible data breach the IT team must be immediately informed who will also inform the Principal and the Data Protection Officer.

If a learner becomes aware of a possible data breach they should inform a member of staff who will immediately inform the Academy Principal.

For any data breach the email address ITsecurity@southstaffs.ac.uk should be used.

Should a data breach occur the Principal will undertake a full and immediate risk assessment with regard to reputational, financial and operational risk. Where the breach is notifiable to the ICO the Principal will be responsible for reporting the breach within the required timescales. The nature and scale of the breach will determine how an individual is contacted to advise that their data may have been compromised. A Communication plan will be implemented, depending on the individual circumstances of a breach, which will include any PR arrangements required to minimise the impact on individuals and the organisation.

3.10 **Data Protection by Design**

The Academy must adopt a privacy by default model when it comes to data handling and processing. Privacy by design is now a legal requirement of the GDPR under the term 'data protection by default and design'.

The Rural Enterprise Academy designates a Data Protection Officer. The nominate person will be responsible for the following. The name of the DPO will be made available to all stakeholders and any change of designated person will be notified as soon as possible.

It is a requirement of the GDPR that the Data Protection Officer has the knowledge, support and authority to conduct the role effectively.

It is the responsibility of the Data Protection Officer to:

- Keep the Board updated about data protection responsibilities, risks and issues.
- Review all data protection procedures and policies on a regular basis.
- Provide appropriate briefings and information, advice and guidance on data protection for all staff members and those included in this policy.
- Respond to questions on data protection from staff, Board members and wider stakeholders.
- Respond to individuals such as clients and employees who wish to know which data is being held that relates to them at The Rural Enterprise Academy.
- Check and approve with third parties that handle the company's data any contracts or agreement regarding data processing.
- The Data Protection Officer has daily operational responsibility for the implementation of this policy.

4 General Requirements

4.1 Key sensitive/special category data covered by the GDPR relates to:-

- Race
- Gender
- Politics
- Religion
- Health
- Trade Union membership
- Criminal Record data
- Genetic and biometric data

4.2 The only people able to access data covered by this policy should only be those who require that access to conduct their work.

4.3 Employees must keep all data secure by taking sensible and appropriate precautions some of which are highlighted below:

- **Strong passwords must be used and never shared.**
- **Personal data must never be disclosed to anyone unauthorised to access it.**
- **Data should be regularly reviewed and updated if it is found to be out of date. If the data is no longer required for the purposes of the organisation, it should be disposed of safely.**

- **Employees should request advice and guidance in regard to any data protection assistance from the Academy Data Protection Officer.**

- **Where personal information is stored on paper, it should be kept in a secure place that would reasonably prevent any unauthorised person from accessing it easily and in a location where others cannot see it.**

- **Paper printouts containing personal information must not be left in a location where any unauthorised person might be likely to see it, such as on a printer/photocopier.**

- **Paper printouts containing personal information should be shredded and disposed of securely when no longer required.**

- **Electronic data must be stored securely and reasonably protected from unauthorised access, accidental deletion or malicious cybercrime.**

- **Removable storage media should not be used in the Academy as the organisation has infinite cloud storage provided by Google which is fully GDPR compliant. In the exceptional circumstances requiring the use of removable storage media such as memory sticks, advice must be taken from the Data Protection Officer before use. Only fully encrypted memory sticks will be approved for use and as supplied by the Academy.**

- **Data that just requires storage should only be stored on Google Drive as a fully backed up and GDPR compliant storage solution. Local drives and servers must not be used for this purpose without the permission of the Data Protection Officer.**

- **All data should be backed up (either automatically through Google) or through appropriate disaster recovery mechanisms. Recovery procedures should be tested regularly.**

- **All servers and computing devices processing or containing personal data must be protected by approved security software and a firewall that would provide external scrutiny with assurance of full GDPR compliance.**

- **When working with personal data, all employees must ensure that their computer screens are locked when left unattended.**

- **Personal data should not be shared with informal channels such as an email. An email is not a secure method of communication.**

- **Data that is being transferred outside of the Academy should be encrypted. For advice and guidance the IT Support Team can assist.**

- **Data should be held in as few places as possible and necessary. Staff should avoid creating additional datasets where possible.**

- **Staff should take every opportunity to ensure that personal data is updated. For example by confirming personal details over the phone.**

- **The Academy must ensure that data subjects can easily update the personal information held about them.**

- **Data should be updated as inaccuracies are discovered. This may include a learner or parent that can no longer be reached on the number stored, for example and it should then be removed from the database.**

The Rural Enterprise Academy Data Breach Flow Chart