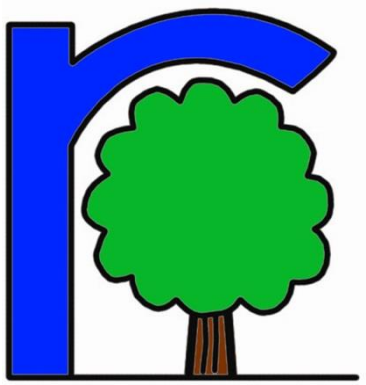
# RADFORD ACADEMY



# Data Protection Policy

This document is a statement of the aims and principles of the School, for ensuring the confidentiality of sensitive information relating to staff, pupils, parents and governors.

| | |
|---|---|
| Definitions (Data Protection Act 1998) *Personal Data* | Data relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. Includes name, address, telephone number, id number. Also includes expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of that individual. |
| *Sensitive Data* | Personal data consisting of information as to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sexual life, criminal convictions. Sensitive data is subject to much stricter conditions of processing. |
| *Data Controller* | A person (or organisation) who determines the purposes for which and the manner in which any personal data is to be processed. |
| *Data Subject* | Any living individual who is the subject of personal data held by an organisation. |
| *Processing* | Obtaining, recording or holding the data or carrying out any operations on the data, including – organisation, adaptation or alteration of the data; retrieval, consultation or use of the data; disclosure of the data by transmission, dissemination or otherwise making available; alignment, combination, blocking, erasure or destruction of the information or data. |
| *Third Party* | Any individual/organisation other than the data subject or the data controller. |
| *Relevant Filing System* | A relevant filing system exists where records relating to individuals (such as personnel records) are held in a sufficiently systematic, structured way as to allow ready access to specific information about those individuals. Personal data as defined and covered by the Act can be held in any format: electronic (including websites and emails), paper- based, photographic etc. from which the individual's information can be readily extracted |

## Introduction

Radford Academy needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. 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, Radford Academy must comply with the Data Protection Principles which are set out in the

Data Protection Act 1998 (the 1998 Act). In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for that purpose.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.

Radford Academy and all staff or others who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the School has developed this Data Protection Policy.

## Status of this Policy

This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the School from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

## The Data Controller and the Designated Data Controllers

The School as a body corporate is the Data Controller under the 1998 Act, and the Governors are therefore ultimately responsible for implementation. However, the Designated Data Controllers will deal with day to day matters.

The Headteacher, the Business Manager and the Administration Assistant are the data controllers in school.

Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the appropriate Designated Data Controller.

## Responsibilities of Staff

All staff are responsible for:

- Checking that any information that they provide to the School in connection with their employment is accurate and up to date.
- Informing the School of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The School

cannot be held responsible for any errors unless the staff member has informed the School of such changes.

If and when, as part of their responsibilities, staff collect information about other people (e.g.about a student's work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines set out in this policy

## Data Security

All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely.
- Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

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

Care should be taken to ensure that computer screens are visible only to authorised staff and that computer passwords are kept confidential. Computers should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised personnel.

Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as 'confidential waste'. Hard drives of redundant computers should undergo secure electronic deletion before disposal.

This policy also applies to those who process personal data 'off-site'. Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff should take particular care when processing personal data at home or in other locations outside the school.

## Personal information should:

- Be kept in a locked filing cabinet, drawer, or safe; or
- If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up; and
- If a copy is kept on a diskette or other removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

## Rights to Access Information

All staff, parents and other users are entitled to:

- Know what information the School holds and processes about them or their child and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what the School is doing to comply with its obligations under the 1998 Act.

Upon request, the school will provide all staff and parents and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the School holds and processes about them, and the reasons for which they are processed.

All staff, parents and other users have a right under the 1998 Act to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should request this in writing and submit it to the Designated Data Controller.

The School aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days, as required by the 1998 Act.

## Subject Consent

In many cases, the School can only process personal data with the consent of the individual. In some cases, if the data is sensitive, as defined in the 1998 Act, express consent must be obtained. Agreement to the School processing some specified classes of personal data is a condition of acceptance of employment for staff. This includes information about previous criminal convictions.

Jobs will bring the applicants into contact with children. The School has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job. The School has a duty of care to all staff and students and must therefore make sure that employees and those who use School facilities do not pose a threat or danger to other users. The School may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes. The School will only use this information in the protection of the health and safety of the individual, but will need consent to process this data in the event of a medical emergency, for example.

## Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, or race. This may be to ensure that the School is a safe place for everyone, or to operate other School policies, such as the Sick Pay Policy or the Equal Opportunities Policy. Because this information is considered **sensitive** under the 1998 Act, staff (and students where appropriate) will be asked to give their express consent for the School to process this data. An offer of employment may be withdrawn if an individual refuses to consent to this without good reason.

## Publication of School Information

Certain items of information relating to School staff will be made available via searchable directories on the public Web site, in order to meet the legitimate needs of researchers, visitors and enquirers seeking to make contact with the School.

## Retention of Data

The School has a duty to retain some staff and student personal data for a period of time following their departure from the School, mainly for legal reasons, but also for other purposes such as being able to provide references or academic transcripts. Different categories of data will be retained for different periods of time.

## Disposal of Records

Personal data must be disposed of in a way that protects the rights and privacy of data subjects

(e.g. shredding, disposal as confidential waste, secure electronic deletion).

## Conclusion

Compliance with the 1998 Act is the responsibility of all members of the School. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or even to a criminal prosecution.

This policy prepared by Meeta Dave February 2015

Signed Alan Clark (Chair Of Governors)

Date of review January 2016