Category	Security		
Document Name	Data Security & Retention Policy		
Accountable Body	RADIUS		
Reference	SY.P1	**Date Ratified**	10th April 2014
Version	2.3	**Last Update**	26th November 2015

Related Documents

Document	Reference
Data Retention Protocol	SY.P1.T1

Reference Material

Guidance
Data Protection Act 1998

1. Policy Statement

RADIUS and each school are required to process relevant personal data regarding its employees and its pupils as part of its operation. RADIUS complies with the Data Protection Act 1998 and any subsequent relevant legislation, to ensure that all personal data is treated in a manner that is fair and lawful. RADIUS is committed to data security & protection and respects the individual's rights in relating to all matters surrounding data protection.

2. Scope

This policy applies to all staff employed by RADIUS, its volunteers and helpers and pupils attending RADIUS schools. Data covered by this policy includes all personal information, including facts and opinions, held within RADIUS and at each school relating to an individual staff member or pupil.

3. Principles

RADIUS and each school shall so far as is reasonably practicable comply with the Data Protection Principles ("the Principles") contained in the Data Protection Act to ensure all data is:

- Fairly and lawfully processed;
- Processed for a lawful purpose;
- Adequate, relevant and not excessive;
- Accurate and up to date;
- Not kept for longer than necessary;
- Processed in accordance with the data subject's rights;
- Secure;
- Not transferred to other countries without adequate protection.

4. Exemptions

Certain data is exempted from the provisions of the Data Protection Act which includes the following;

- The prevention or detection of crime
- The assessment of any tax or duty
- Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon RADIUS

Radius Trust
Registered Charity Number: 1039938
Company Registration Number: 2919225
Registered Office: Trust Office,
Horsham Road, Grafham, Bramley,
Guildford, Surrey GU5 0LH

5. Responsibilities

Trustees have overall responsibility for ensuring that the organisation fulfils its legal obligations under the Data Protection Act. The CEO is the designated Data Protection Officer for RADIUS.

The Headteacher/Principal of each school is required to ensure that all personal data is processed in compliance with this policy and the Principles of the Data Protection Act 1998.

6. Implementation

RADIUS and each school are required to implement appropriate IT policies and Data Protection & Security procedures to ensure, as far as is reasonably practicable, that personal data is secure, accurate, relevant and processed in accordance with Data Protection Principles.

RADIUS requires each school to be responsible for maintaining its own operational procedures (including induction and training) to ensure good data protection practise is established and followed. Managers must ensure that the Data Protection Officer is informed of any changes in their use of personal data that might affect the organisation's notification.

All staff and volunteers are required to read, understand and accept any policies, protocols and procedures that relate to the personal data they may handle in the course of their work. For the sake of these policies and procedures, the use of the word 'staff' includes both paid staff and volunteers. Breech of this policy may result in disciplinary action which may lead to dismissal.

6.1. Accuracy of Data

RADIUS and its schools ensure that all personal data held in relation to an individual is accurate. Pupils must notify the Headteacher/Principal of any changes to information held about them. An individual has the right to request that inaccurate information about them is erased or corrected.

6.2. Confidentiality

Only specific roles within the organisation are granted access to specific types of highly confidential data, for example medical records, child protection records or personal financial records. Staff are only granted access to confidential information if it is necessary for them to perform their professional duties.

7. Pupil Data

7.1. Personal Data

Personal data covers both facts and opinions about an individual. Each school may process a wide range of personal data of pupils, their parents or guardians as part of its operation. This personal data may include (but is not limited to); names and addresses, bank details, academic, disciplinary, admissions and attendance records, references, examination scripts and marks.

7.2. Processing of Personal Data

RADIUS requires each school to obtain consent for the processing of personal data unless the processing is necessary for the school to undertake its obligations to pupils and their parents or guardians. Any information which falls under the definition of personal data, and is not otherwise exempt, remains confidential and is only disclosed to third parties with the consent of the appropriate individual or under the terms of this policy.

7.3. Sensitive Personal Data

A Trust school may, from time to time, be required to process sensitive personal data regarding a pupil, their parents or guardians. Sensitive personal data includes medical information and data relating to

religion, race, or criminal records and proceedings. Where sensitive personal data is processed by the school, RADIUS expects each school to obtain the explicit consent of the appropriate individual in writing.

7.4. Parent/Carer Consent

The rights under the Data Protection Act are the individual's to whom the data relates. However, RADIUS requires each school in most cases to rely on parental consent to process data relating to pupils unless, given the nature of the processing in question, and the pupil's age and understanding, it is unreasonable in all the circumstances to rely on the parent's consent. Parents should be aware that in such situations they may not be consulted.

RADIUS expects each school to only grant the pupil direct access to their personal data if in the school's reasonable belief the pupil understands the nature of the request and the school believes that the data would not be emotionally harmful to the pupil.

Pupils agree that a Trust School may disclose their personal data to their parents or guardian. However, where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or guardian, RADIUS requires each school to maintain confidentiality unless it has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding their consent or if it is a safeguarding and child protection concern and the school believes disclosure is in the best interests of the pupil or other pupils.

7.5. Rights of Access

Pupils have a right of access to information held by RADIUS or the school. Any pupil wishing to access their personal data should put their request in writing to the Headteacher/Principal. RADIUS expects each school to respond to any such written requests as soon as is reasonably practicable and in any event, within 40 days for access to records and 21 days to provide a reply to an access to information request.

Certain data is exempt from the right of access under the Data Protection Act this may include information which identifies other individuals, information which the school reasonably believes is likely to cause damage or distress, or information which is subject to legal professional privilege. The school is also not required to disclose any pupil examination scripts.

RADIUS expects each school to treat as confidential any reference given by the school for the purpose of the education, training or employment, or prospective education, training or employment of any pupil. RADIUS requires each school to acknowledge that an individual may have the right to access a reference relating to them received by the School. However such a reference is only disclosed if such disclosure does not identify the source of the reference or where, notwithstanding this, the referee has given their consent or if disclosure is reasonable in all the circumstances.

7.6. Disclosure of Information

The data that each school holds is only used or passed on for specific purposes allowed by law. Occasionally, a RADIUS school may pass personal data (including sensitive personal data where appropriate) to third parties, including local authorities, other public authorities, health professionals and the school's professional advisers, who will process the data:

- to enable the relevant authorities to monitor the school's performance;
- to compile statistical information (normally used on an anonymous basis);
- to secure funding for the school (and where relevant, on behalf of individual pupils);
- to safeguard pupils' welfare and provide appropriate pastoral (and where relevant, medical and dental) care for pupils;
- where specifically requested by pupils and/or their parents or guardians;

- where necessary in connection with learning and extra-curricular activities undertaken by pupils;
- to enable pupils to take part in national and other assessments and to monitor pupils' progress and educational needs;
- to obtain appropriate professional advice and insurance for the school;
- where a reference or other information about a pupil or ex-pupil is requested by another educational establishment or employer to whom they have applied;
- to disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips;
- where otherwise required by law, for example in connection with the government's ContactPoint and Connexions services; and
- otherwise where reasonably necessary for the operation of the School.

Where the School receives a disclosure request from a third party, RADIUS requires each school to take reasonable steps to verify the identity of that third party before making any disclosure.

7.7. Use of Personal Information by The School

RADIUS Schools' are permitted to occasionally make use of personal data relating to pupils, their parents or guardians in the following ways.

- To make use of photographic images of pupils in school publications and on the school website. However, RADIUS requires each school to not publish photographs of individual pupils with their names on the school website without the express agreement of the appropriate individual.
- For fundraising, marketing or promotional purposes and to maintain relationships with pupils of the school, including transferring information to any association society or club set up for the purpose of establishing or maintaining contact with pupils or for fundraising, marketing or promotional purposes.

7.8. Security

RADIUS expects each school to take reasonable steps to ensure that only members of staff have access to personal data relating to pupils, their parents or guardians where it is necessary for them to do so. All staff are made aware of this policy and their duties under the Data Protection Act. RADIUS requires each school to ensure all personal information is held securely and is not accessible to unauthorised persons.

7.9. Enforcement

If an individual believes that the school has not complied with this policy or acted otherwise than in accordance with the Data Protection Act, they should utilise the school's complaints procedure and should also notify the Headteacher/Principal.

8. Staff Data

8.1. Personal Data

RADIUS complies with the Data Protection Act 1998 (DPA) which regulates the way in which certain information about employees is held and used. The policy gives some useful information about the type of information that the organisation keeps about its employees and the purposes for which it keeps them.

Throughout employment and for as long a period as is necessary following the termination of employment, RADIUS and each school need to keep information for purposes connected with an employee's employment, including recruitment and termination information.

This information is normally stored in an employee's file and may include:

- Applications forms and CV's
- Interview records
- DBS records (not DBS check), references and other pre-employment vetting checks
- Offers of employment
- Disciplinary and Grievance records
- Contracts of Employment
- Performance management reviews
- Probationary Reviews
- Supervision records
- Notes of informal meetings and interviews
- Relocation details
- Allowances and expenses
- Training and qualification details
- Salary, additional payments and bonuses etc
- Work permits
- Pension records
- Holiday records
- General HR correspondence
- Attendance records and absence management
- Medical and Occupational Health reports (in separate OH file)
- Self Certification and Medical certificates (in separate OH file)

RADIUS and each school do not include data or other material that cannot legitimately be shown to be related directly or indirectly to the employment of the employee concerned.

The information held is for senior management and administrative use only, but from time to time, RADIUS may need to disclose some information we hold about employees to relevant third parties (e.g. where legally obliged to do so by the HM revenue and Customs service). RADIUS may also transfer information to another group or organisation, solely for purposes connected with an employee's career or the management of RADIUS or it's schools.

It should be noted that RADIUS and each school might hold the following information about an employee for which disclosure to any person will be made only when strictly necessary for the purpose set out below:

- An employees health, for purposes of compliance with RADIUS's Health and Safety obligations
- For the purpose of personnel management and administration, for example to consider how an employee's health affects his or her ability to do his or her job and, if the employee is disabled, whether he or she requires any reasonable adjustment to be made to assist him or her at work
- The administration of insurance, pension, sick pay, and any other related benefits in force from time to time
- In connection with unspent convictions to enable us to address an employee's suitability for employment.

RADIUS requires all employees to comply with the DPA in relation to the information about other staff. Failure to do so, e.g. unauthorised, inappropriate or excessive disclosure of or obtaining information about individuals, is regarded as serious misconduct and will be dealt with in accordance with RADIUS's disciplinary policy and procedure. If an employee is in a position to deal with personal information about other employees, they are given separate guidance on their obligations, and are required to seek advice if they are unsure.

The person with overall responsibility for compliance with the DPA is RADIUS's CEO.

8.2. Rights Of Access

Employees have right of access to their personal employment record normally **within one month** of written notice being received by RADIUS. If a telephone request for access is received the caller must be notified that the request should be put in writing. ***In response to a request, the appropriate Manager receiving the access request is required to confirm, in writing, the date, time and place at which access will be provided.***

Where possible live data, e.g. copies of current emails and camera footage, should be presented to the employee. However, it is reasonable for **the Data Controller** to ask for further information from the Data Subject in order to assist in locating this type of employee data. This could include the dates, email subjects, locations and the times the footage was recorded. The Data Protection Act states that if the Data Controller needs further information in order to locate the information which the subject seeks and has told the Data Subject this, then the Data Controller can wait until this information is received before the 40 day time limit begins.

Archived data or data that is very difficult or burdensome to locate need not be retrieved if the likely effect of non-retrieval is minimal on the data subject.

Details Of Access

Access is by prior arrangement and viewing of the contents of the record is at its stored location, in the presence of a person nominated by the HR Manager. (The sole purpose of this provision is solely for the purposes of ensuring that no material is inappropriately removed or destroyed).

All access to documents and data is recorded and kept by the HR Manager.

Copies Of Records

Employees may, within reason, request one copy of any or all of documents held on a data subject if they wish. A record is made of any copies requested and **where possible,** provided, including date and place together with the name of the person providing them.

8.3. Confidentiality of Third Parties

The Charity Office – Office manager and Headteachers / Principal of schools are responsible for ensuring that any data containing third parties complies with the duty of confidentiality. This may include blurring images on tapes, deleting references to specific individuals or third parties in emails and in the event that the third party cannot be disguised it is the Trust's manager's responsibility to get written consent to disclose his/her identity.

8.4. Accuracy Of Data

An employee may challenge the accuracy of an entry in the record and where, on investigation, it is found to be inaccurate shall be entitled to have the entry corrected or removed, whichever is the most appropriate and to have this action confirmed in writing as having been done.

8.5. Legitimacy Of Data

An employee may challenge the legitimacy of making or keeping particular data or other information in the record.

Exercising The Right To Challenge The Accuracy Or Legitimacy Of An Entry

- If an employee believes that the data held on them is inaccurate then they should approach either the Data Controller or the HR Manager.

- At all stages, any decision shall be taken in consultation with the appropriate HR Advisor and all reasons shall be given to the employee so that they understand the decision taken. The employee will receive written response within 21 days stating what action has or will be taken or stating the reasons for regarding the concerns as unjustified.
- If the employee is still not satisfied they must refer the matter to the HR Manager/Data Controller for investigation.

8.6. Recruitment

Interviews

Interview notes are made and retained for each applicant, reflecting their answers to the set of questions described above. These notes are retained by RADIUS for a period of 12 months for external candidates following the interview and then destroyed. Interview notes for internal candidates are kept on the personnel file for the duration of their employment and for 6 years after employment.

Retention Of Recruitment Records

At the end of the recruitment process, all records are kept by RADIUS and each school for 12 months in case of requests for feedback or possible litigation.

References

RADIUS only obtains references once the applicant has given their permission to do so, which is requested on the application form. References are requested in writing from the applicant's previous two places of employment, or from the applicant's school or college if they have not worked for two employers.

9. Security Arrangements

RADIUS has identified three levels of data security; throughout this policy these are referred to as 'Level 1', 'Level 2' and 'Level 3'. These levels include, but are not limited to, the following:

Level	Data	Security
'Level 1' Highly Secure Data	• Medical Records • Child Protection Records • Disclosures • Allegations • Complaints • Personal Finance	For information held in an electronic format, this data is VLAN secured from pupil accessible areas. Such data is not held on either personal or portable computers. Where it is necessary to transmit such data to external parties, files are encrypted and/or password protected. Level 1 paper records are secured behind two locked doors with access restricted to authorised personnel only. Copies are only to be taken under strict supervision. Where it is necessary to forward information to external organisations, this is always by hand or secure courier and 'proof of receipt' is always obtained.
'Level 2' Secure Data	• Pay • Pension • Absence Records • Performance Managements • Attainment	For the majority of information held in an electronic format, this data requires username and password authentication and is VLAN secured from pupil accessible areas. Where it is necessary to transmit such data to external parties, files are encrypted and/or password protected. Paper records are secured behind a locked door.
'Level 3' Private Data	• Name • Address • UPN • Contact Details	For information held in an electronic format, this data is username and password protected. Where it is necessary to transmit such data to external parties, files are encrypted and/or password protected.

9.1. Business Continuity

All electronic data is backed up every night and stored in a secure location in a different building to the server room. The CEO will ensure arrangements are in place for IT competent employees or agents to access data and files as necessary.

9.2. Access To Data

RADIUS requires all requests for access to pupil related Level 1 information to be directed to the Headteacher / Principal / Lead Designated Safeguarding & Child Protection Officer of the relevant school. All requests for access to Staff related Level 1 information is directed to the HR manager or Charityy Office – Office Manager at RADIUS.

Access to Level 2 and Level 3 data is at the discretion of the manager holding the data on the basis of 'as necessary' in order for staff to fulfil their duties.

Granted/permitted access requests for electronic data is forwarded to the RADIUS IT Department who will provide access on a permanent, semi-permanent or supervised basis depending on the request. Staff members who require access to Level 1, Level 2 or Level 3 data whilst off site are supplied with secure remote access via VPN access.

RADIUS acknowledges that all electronic data held is accessible by approved personnel cleared for access by the CEO.

Information is not to be released to a 3rd party without the written consent of the individuals concerned, unless RADIUS are obliged to do so by its statutory obligations.

9.3. Data Recording & Storage

9.3.1. Electronic Data

Staff and Pupil computer accounts (including emails and personal documents) are archived onto a dedicated backup tape approximately 4 weeks after they leave. This information is accessible by CEO approved Trust personnel or agents who can grant access to others if required.

The majority of Level 1, Level 2 and Level 3 data for both Staff and Pupils are held within electronically in a secure database application. Paper records are secured in locked storage with controlled access via key individuals, CEO, HR Manager or Headteacher/Principal as appropriate..

Staff and pupil records are held indefinitely in order to satisfy all legal obligations.

9.3.2. Paper Records

RADIUS expects each school to ensure that paper records are held securely and protected from loss arising from theft, fire, flood or other risk. RADIUS maintains separate storage facilities for its records. Archived paper documents are indexed in such a way that;

- They can be readily retrieved should there be a need to do so
- They can be securely destroyed when it is required