RED ROSE SCHOOL DATA PROTECTION POLICY & PRIVACY NOTICE

Section 7

6

Updated: November 2019

School's authorised officer: Gill Makinson

Policy Statement (1)

Red Rose School is mindful of national guidance for schools on Data Protection and related issues from the Information Commissioner's Office (ICO). As technology evolves, the school continues to endeavour to take into account the core principles of the Data Protection Act, that personal data:

- Is processed fairly and lawfully
- Is obtained only for lawful purposes and is not further used in any manner incompatible with those original purposes
- Is accurate and, where necessary, kept up to date
- Is adequate, relevant, and not excessive in relation to the purposes for which it is processed
- Is not kept for longer than is necessary for those purposes
- Is processed in accordance with the rights of data subjects under the Data Protection Act
- Is protected by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage
- Is not transferred to a country or territory outside of the European Economic Area, unless that country or territory ensures an adequate level of protection of the personal information.

Policy Statement (2)

- This policy applies to all members of the School community
- The School implements this policy through adherence to the procedures set out in the rest of this document
- This policy is made available to all interested parties in accordance with our *Provision of Information* policy. It should be read in conjunction with the following policies: *Provision of Information*, *Social Media, and ICT Acceptable Usage.*
- The school is fully committed to ensuring that the application of this policy is non-discriminatory in line with the Equality Act (2010).
- This policy is reviewed at least annually, or as events or legislation changes require

- The deadline for the next review is no later than 12 months after the most recent review date indicated above.

Personal Data

Personal data is understood to be any data that can be used to identify a pupil, parent, or member of staff. It includes any photographs taken by staff of pupils for school purposes.

In more detail, personal data is information which relates to an identifiable living individual that is processed as data. Processing means collecting, using, disclosing, retaining, or disposing of information. The data protection principles apply to all information held electronically or in structured files that tells something about an identifiable living individual. The principles also extend to all information in education records. Examples would be names of staff and pupils, class lists, dates of birth, addresses, national insurance numbers, school assessment and homework marks, medical information, exam results, SEN assessments and staff development reviews.

Sensitive personal data is information that relates to race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, gender and criminal offences.

The school recognises the differences between processing personal data and sensitive personal data, and that there are greater legal restrictions on the latter. For example: the Head Teacher's identity is personal information but everyone would expect it to be publicly available; however, the Head Teacher's home phone number would usually be regarded as private information.

The ICO document 'Definitions of Personal Data' provides comprehensive definitions.

Biometric Data
The school does not hold any biometric data on pupils or staff.

Security 1 – Access
The School building is accessible only by key and fob entry pad. All visitors are managed in accordance with safeguarding regulations.

Security 2 – CCTV
The School uses CCTV cameras in appropriate locations, externally and internally, purely for the purposes of campus security. Images are held for 14 days and then deleted, if not required. The images can be accessed only by authorised security personnel.

Security 3 – Protection
All personal data stored on school campus, including hard copy, and on removable media such as DVDs and CDs, is secured in locked units or offices or both when not in use.

Security 4 – Back-Up
The school system is backed up each week night and also weekly, and storage is secure and local.

Passwords & Basic Security

- Staff must follow the password guidance in Appendix 1 with regard to access to, and protection of, all school-based personal data
- If staff access their professional emails on a mobile device, staff must ensure that these devices have a strong password applied. If the mobile device does not permit a strong password, then every effort should be taken to make the access code as strong as possible
- It is also advised to delete professional emails, messages and any attachments that have been viewed from the mobile device, as soon as possible after reading
- Staff must never allow anyone, including pupils or family members, to use their login credentials to access school resources or the internet, even if it is for only a few minutes, or if 'they log them in'
- Staff are not only authorised to temporarily hold professional personal data on memory sticks, laptops or the like, but any device which holds personal data about any employee or pupil must be encrypted. Guidance on encryption is available from the Data Manager; and staff must know how delete these files once they have been finished with in such a way that they may not be recovered or hacked
- Staff are not permitted to store any professional personal data on home PCs or similar. If staff may receive any professional personal data, for example in an email, on their personal home account, they should permanently delete any such communications, including attachments, once read. Any such PCs or systems must also be protected by a strong password
- Any member of the school community who has held or received sensitive data on a home computer, smart phone, flash drive or other device should be aware that such data can sometimes be recovered; the school offers the opportunity to wipe such devices securely before they are disposed of or sold
- Any professional personal data in hard copy must be handled with the highest degree of appropriate care and sensitivity. Staff are required to be particularly mindful, if ever hard copy must be transported off the school campus, including:
    - Senior staff acting as emergency contact for school trips
    - Teacher's planners etc, if they contain class lists and pupil data
    - Relevant school resources for external meetings or conferences

  All hard copy documents should be securely stored or shredded as soon as possible following use.
- Leaders on any school trips and visits must complete a Data Protection Risk Assessment, showing that every effort has been made to manage the sensitive data they will be carrying as appropriately as possible (*see Appendix 3*)

- Staff must also be mindful when communicating by email or fax that the addressees are correct, and that the protection of professional personal data is not compromised
- Staff must ensure that they never leave a terminal unsecured, which could allow unauthorised access to professional data.

Pupil, Staff & Proprietors' Data

- All pupil personal data, including contact and billing information, is initially collated as part of the admissions process
- Pupil information that is relevant to all teaching staff is accessible through the *gDrive,* which is password protected, and as hard copy in cupboards, which are locked when not in use
- Copies of pupil personal data, such as regulatory medical lists in staff areas, are positioned in discreet locations away from external view, and these areas have restricted or supervised access beyond the working day
- All staff personal data, including emergency contact and relevant medical information, is collated and updated by the School Administrator; this data is stored on the central system with limited access only to personnel authorised by the Head Teacher
- Staff records, including application forms and professional review documents, are stored in the school safe in the Head Teacher's office
- The school does not include any personal addresses, emails, telephone numbers, fax numbers on video, on the website, in a prospectus or in other printed publications, without the express permission of the individual
- If a pupil leaves to attend another school, their Pupil File will be transferred to the new school.

Images & Photographs of Pupils 1 – Context

The ICO states that the Data Protection Act is unlikely to apply in most cases where photographs or videos are taken in schools and other educational institutions. If photos or videos are taken for personal use they are not covered by the Act; however, photographs or videos taken for official school use (eg. publicity, assessment evidence, ID data) will be covered by the Act.

Examples of Personal use:

- A parent takes a photograph of their child and some friends taking part in the school Sports Day to be put in the family photo album. These images are for personal use and the Data Protection Act does not apply
- Grandparents are invited to the school nativity play and wish to video it. These images are for personal use and the Data Protection Act does not apply.

Examples of Official use:

- Photographs of pupils or students are taken for building passes. These images are likely to be stored electronically with other personal data and the terms of the Act will apply
- A small group of pupils are photographed during a science lesson and the photo is to be used in the school prospectus. This will be personal data but will not breach the Act as long as the children and/or their guardians are aware this is happening and the context in which the photo will be used.

Examples of Media use:

- A photograph is taken by a local newspaper of a school awards ceremony. As long as the school has agreed to this, and the children and/or their guardians are aware that photographs of those attending the ceremony may appear in the newspaper, this will not breach the Act.

The School informs parents about the possible use of images of pupils, and parents may refuse to give their consent. Additionally, the school sends out annually a separate statement, which also includes possible use of images in the media; again, parents may refuse to give their consent. Any refused consent is recorded by the school Registrar and a list is circulated to staff for their information (*Appendix 2*).

It is understood that school procedures in relation to images of pupils support both data protection requirements as well as professional safeguarding procedures, as appropriate.

Images & Photographs of Pupils 2 – School Events

The school permits visiting families to take personal photographs or videos at school events. However, the school explicitly advises; either in accompanying literature for the event or in an announcement at the start; that photographs or videos are for personal use only, which includes not uploading the images onto social media or the like. The right to withdraw consent will be maintained and any photography or filming on campus will be open to scrutiny at any time. Parents may contact the school to discuss any concerns regarding the use of images.

Images & Photographs of Pupils 3 – Practice

- The Head Teacher is responsible for ensuring that all employees are aware of procedures and requirements for the acceptable, safe use and storage of all camera technology and images within the school
- All photographs for official school use are stored on the central system in the main office. No photographs or images should be stored anywhere else on the school system

- Images are disposed of when they are no longer required; they are returned to the parent or carer, deleted and wiped or shredded as appropriate. Copies are not to be taken of any images without relevant authority and consent from the Head Teacher
- All members of staff (including volunteers) will ensure that all images are available for scrutiny and will be able to justify any images in their possession
- Only school-owned equipment (e.g. school provided digital or video cameras) are used by staff to capture images of pupils for official purposes. Use of personal cameras or devices by staff is permissible only with line management authorisation, and any images must be transferred to the school system at the earliest opportunity and permanently deleted from the personal device. Equally, personal equipment may be used with authorisation, if a school-owned memory card is inserted for the unique use of official school photography, although the handling of the images will be as above.
- Any apps, websites or third-party companies used to share, host or access pupils' images must be approved by school management prior to use
- Pupils must be suitably dressed for any photograph, and any images or videos that include children are selected carefully
- Pupils' full names are not used in association with photographs on the website or in school publications for whom the school remains responsible
- The school will discuss the use of images with children and young people in an age appropriate way, where applicable
- Members of staff may take photographs of pupils (eg. a class group at the end of an academic year) for personal reasons, but the pupils must be in agreement at the time and it would not be advisable for staff to photograph individual pupils in this way
- A child or young person's right not to be photographed is to be considered, if relevant to the given situation
- Photography is not permitted in sensitive areas such as changing rooms, toilets, swimming areas and the like
- If video technology is used to record all or part of a lesson for professional purposes, pupils must be informed beforehand and the rationale explained. Subsequent use of the images is bound by the consent and storage procedures of this policy, and due care must always be taken where any pupil may be identified by name. No image should ever be used that may be considered to be disrespectful or unprofessional with regard to any pupil
- If video technology (eg. webcam) is used within a lesson, which involves the filming of any pupil or pupils, verbal consent must be sought and agreed beforehand. A pupil may refuse to be filmed and, in this situation, this must be respected. The use and storage of all such images are bound by the principles and practices of this policy

- Where a press photographer is invited to celebrate an event:
    - Every effort is made to ensure that the newspaper's (or other relevant media) requirements can be met
    - A written agreement is sought between the school and the press which will request that a pre-agreed and accepted amount of personal information (e.g. first names only) can be published along with images and videos. Note that the school may have to accede to a newspaper's procedures on this matter, if only full names are published
    - The identity of any press representative will be verified and access will only be permitted where the event is planned, and where press are to be specifically invited to attend
    - No authorisation is given to unscheduled visits by the press under any circumstances
    - Every effort will be made to ensure the press abide by any specific guidelines should they be requested
    - No responsibility or liability however can be claimed for situations beyond reasonable control, and where the school is to be considered to have acted in good faith
- Where a professional photographer is engaged to record any events:
    - They will be prepared to work according to the terms of the School's e-Safety procedures
    - They will sign an agreement which ensures compliance with the Data Protection Act and that images will only be used for an agreed specific purpose.

Website

The school website has a Privacy Policy. Images of pupils are used with general permission, and the school is mindful, where possible, to protect individual identities and other personal data, such that they may not be abused by a malicious external party. If pupil names are given, first names only are used.

Online Storage

- Online storage refers to services such as Microsoft Cloud services, gDrive, iCloud and DropBox, for example
- Unless explicitly stated, the school does not assume that data uploaded to an online storage area is within the European Economic Area; therefore, no personal data should be stored using any online services, where the storage area is not thus clarified
- If the online storage area states explicitly that it holds the data within the European Economic Area, personal data could be stored in this location if the Network Manager has ascertained that:
    - a strong password is used to access the account

    - the data stored, using these services is encrypted using approved technology
    - the locations the data is replicated to is documented in a risk assessment
    - the data is not accessible to others outside of the School or those not authorised to access that data
- Any data held in these online storage services may be subject to access or Freedom of Information requests; thus the school must be aware of what general data is held in these locations
- The Network Manager reviews authorised use of online storage to ensure that practice adheres to the above, and all staff must liaise with the Network Manager before they employ any online storage service.

Staff Turnover

When a member of staff leaves the school:

- Access to emails and school databases is suspended as soon as the final date of contracted employment has passed
- The member of staff must ensure that any professional personal data in online storage services is deleted, or control of access is forwarded to a colleague.

Disposal of Data

The school provides shredding facilities and a secure bin for the safe disposal of confidential documents in the main office.

Training of Staff

Staff receive updates on data protection and appropriate advice at least annually, as well as part of their regular safeguarding training.

Useful Documents

The school has copies of the following supporting documents on the local gDrive:

1) ICO_Data Protection Guidance for Schools (2012)
2) ICO_CCTV Code of Practice (2008)
3) ICO_Definitions of Personal Data (2007)
4) ICO_Dealing With Subject Access Requests (2007)
5) ICO_Freedom of Information Guide (2013)
6) ICO_Bring Your Own Device Guidance (2013)
7) BECTA_Keeping Data Safe and Secure
8) RMS_Records Management Information [*Timescales for data retention*]

Appendix 1: E-Security Guidance

Staff 'Log-on' passwords must be kept secure and confidential at all times, in order to protect the confidentiality of the information stored on school systems. Each member of staff must ensure that their log-on password is **strong'** (see below).

Computers must never be left unattended and logged-on, if pupils can access it - always lock your machine when you are away from it ('Ctrl-Alt-Del'; 'Lock Computer'). It is also advisable to have the projector on 'no show' when you do type in your details to log on, just in case you inadvertently type your password onto the 'Username' line.

Keys to password strength: length and complexity

An ideal password is long and has letters, punctuation, symbols, and numbers.

- Whenever possible, use at least 8 characters or more
- The greater the variety of characters in your password, the better
- Use the entire keyboard, not just the letters and characters you use/see most often.

For example, an appropriate password for an English colleague may be as follows:

- Consider a familiar line of text, such as "Shall I compare thee to a summer's day?"
- Reduce it to first letters, keeping a mixture of upper and lower case: SIcttasd
- Include the punctuation and insert numbers: S1ct2asd?
- To increase this 'medium strength' password to 'strong' add the date of the sonnet and the number: 1609S1ct2asd?S18

Common password pitfalls to avoid

Cyber criminals use sophisticated tools that can rapidly decipher passwords. Avoid creating passwords using:

- **Dictionary words in any language.** Words in all languages are vulnerable
- **Words spelled backwards, common misspellings, and abbreviations.** Words in all languages are vulnerable
- **Sequences or repeated characters.** Examples: 12345678, 222222, abcdefg, or adjacent letters on your keyboard (qwerty)
- **Personal information.** Your name, birthday, driver's license, passport number, or similar information.

Test the strength of your password by clicking this link
https://www.my1login.com/resources/password-strength-test/

Appendix 2: Statement to Parents

Dear Parents

As a school, we take our responsibilities with regard to Data Protection very seriously and is provided in our local *Data Protection* policy, which is accessible on the School Website.

One important element of this concerns what we do with photographs or videos of pupils, taken for school purposes. We currently assume automatic consent as below, and if you are content with this, you need do nothing further and return nothing to us:

- The school may use photographic or video images of your son/daughter, taken for school purposes, in school publications, on the school website and other school social media, or other publicity or professional uses. If the school includes your son/daughter's name with the image, the first name only will be used
- The school may permit the press to use photographic or video images of your son/daughter, taken for school purposes, in media publications. In such circumstances, the school is required to provide a full name to the press, and possibly additional details needed for publication.

If, for any reason, you do not wish your consent to one or both of the above to be automatic, we would ask that you put this in writing to the Head Teacher, please. Your wishes in this matter will then be fully respected.

Appendix 3: Risk Assessment Guidance

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions Form (example below):

Staff Name	Personal Data at Risk	Protective Marking of Confidentiality (where relevant)	Detail of Risks	Overall Risk Level (low, medium, high)	Action(s) to minimise Risk

Appendix 4: Data Protection Policy (Privacy Notice)

Scope

The policy and procedure set out in this document applies to all employees; including teaching, support, fixed-term, part-time, full-time, permanent and temporary staff.

This policy is a privacy notice for employees and has been updated to ensure it complies with the requirements of the General Data Protection Regulation and associated data protection laws.

As a values-led organisation our values of ambition, confidence, creativity, respect, enthusiasm and determination are key to our purpose and underpin all that we do.

Responsibility for Data Protection

As part of its everyday activities as your employer, Red Rose School will use or 'process' personal data about you. This policy sets out what personal data we will collect, the purposes for which it is processed and who we may share personal data with.

The Data Controller for all personal information held by the School is the Head Teacher. The School is registered with the ICO. The registration number is Z3113772.

The Data Protection Officer for the School is the Head Teacher.

The Categories of personal data held by the Group about employees are

- Contact details: Names, address, telephone numbers, email addresses and other contact details;
- Recruitment: information in application forms, references, psychometric tests; equal opportunities monitoring; etc.
- Safeguarding checks: The single central record will contain your name, address, DOB, Job title, start date, details of ID provided such as passport numbers and driving licence numbers, qualification checks, teacher number if applicable, notes regarding outcomes of Barred list checks, DBS checks, right to work in UK checks, names of referees and details of any safeguarding training received
- Pay: payroll details; NI number; pension contributions; tax references; bank details; salary etc
- Performance and discipline: performance appraisals, targets and achievements; notes of disciplinary and grievance meetings; disciplinary warnings; etc.

- General HR administration: attendance records; medical reports and records; health and safety accident reports; etc.
- Education and training: education and training records;
- Communication: details in internal directories and newsletters; etc.
- Security: details for pass cards; references; CCTV images; voice recordings; DfE List 99 and Police Checks; the results of Disclosure and Barring Service checks

We also process the following special categories of personal data:

- Ethnicity
- Information regarding trade union membership
- Medical information where this relates to your employment.

The legal basis on which we process this information is:

The legal basis for processing the personal data listed in points above are:

- to enable us to fulfil the terms of your contract of employment
- to enable us to comply with our legal obligations
- where the processing is necessary for the purposes of our legitimate interests as defined in the GDPR.

We will only process the special categories of personal information listed in points above to fulfil our employment law obligations, including compliance with the Equality Act 2010, or, where necessary, for the purposes of occupational medicine, to assess your working capacity.

What will we do with the personal data that we collect

Any information held about you will be held securely on file, (either computer or paper-based) and used only for the purposes described in this document.

We will use your personal data to:

- Pay your salary and expense claims; process pension payments; deal with any queries you may have and make such returns as HMRC may require;
- If deductions are made from your gross salary for benefits or Trade Union subscriptions the details of such deductions will be shared with the relevant organisation;
- Carry out equal opportunities monitoring;
- Carry out and keep records of performance appraisals
- Where applicable carry out investigations and hold disciplinary and grievance meetings in compliance with the relevant policies;
- Carry out general personnel administration: attendance records; medical reports and records; health and safety accident reports;
- Keep records of any education and training that you have completed

- Maintain internal staff telephone and email directories;
- Communicate with you via electronic methods including email and through newsletters;
- Create pass cards
- To carry out our legal obligations to carry out Disclosure and Barring Service Checks (DBS); DfE List 99 and Police Checks; and to confirm that you are entitled to work in the UK;
- Receive and provide references from past and to future employers
- To obtain appropriate professional advice and insurance
- To monitor appropriate use of our IT systems in accordance with the Acceptable Use Policy
- To respond to a request from you regarding your rights under data protection legislation
- For management planning and forecasting
- For statistical research and analysis
- To keep recruitment records and track applicant progress.
- To make use of personal data in aggregate to provide insights into effective school improvement.

Data Retention Periods

We will keep your file until seven years after the termination of your employment.

Data Processors

The use of data processors will only take place if is in compliance with the Data Protection Act 1998 and the General Data Protection Regulation. Decisions on whether we contract with third party processors are subject to a robust approval process and are based on a detailed assessment of the purpose for which the data processing is required, the level and sensitivity of data involved and the arrangements in place to store and handle the data. To be granted access to pupil level data, data processors must comply with strict terms and conditions covering the confidentiality and handling of data, security arrangements and retention and use of the data.

A full list of the data processors used by central office and your school can be found at Annex A. This list will be reviewed and updated on an annual basis.

Sharing Data with third parties (other data controllers)

We will not share your personal data with anyone unless you have asked us to do so or the law and our policies allow us to do so. A list of the data controllers that we share personal information with can be found at Annex B. This list will be reviewed and updated on an annual basis.

Your rights as data subject

Data protection legislation gives individuals certain rights which are detailed below. If you wish to exercise these rights please write to the Head Teacher

Right of access to personal data ‘subject access request’

You have the right to access the personal data that the school holds about you. Requests need to be made in writing. We take the security of personal data seriously so we may ask you for proof of identity to verify that you are entitled to the information requested.

Right to withdraw consent

Where we have obtained your consent to specific processing activities you may withdraw this consent at any time.

Right to rectification

You have the right to have the personal data that we hold about you rectified if it is inaccurate or incomplete. We will respond to such requests within one month.

Right to erasure

You have the right to have personal data erased in certain specific circumstances. If you make such a request we will consider whether the right to erasure applies and give you a full and reasoned response.

Right to restrict processing

In certain circumstances you have the right to request that we restrict the processing of your personal data. If you make such a request we will consider whether the right to restrict processing applies and give you a full and reasoned response.

Annex A

Data processors used by us

MA2 Accountants	Payroll
Microsoft Office 365	Productivity tools e.g. email and word processing
Google Education	gDrive
HMRC	Tax
Local Education Authorities	Pupil Data & Finance

Annex B

Data controllers with whom we share personal data

Payroll Information

We are required to share payroll data with HMRC under section 5 of The Income Tax (Pay As You Earn) Regulations 2003.

If you have requested that deductions are made from your gross pay for trade union subscriptions or employee benefits details of those deductions will be shared with the relevant organisation.

We are required by the Companies Act 2006 and Charities Act 2011 to have our accounts audited annually. As part of this process payroll data is shared with the external auditors. Our current auditors are MA2 Ltd.

School Inspections

Ofsted may have access to information about employees during school inspections.

Department for Education

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment. We are required to share information about our school's staff with the DfE under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Annex C

Department for Education (DfE) Data collection requirements

The DfE collects and processes personal data relating to those employed by schools and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.
The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice and guidance

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.