REDMAIDS' HIGH SCHOOL
FOR GIRLS | BRISTOL

DATA PROTECTION POLICY

Introduction

1 **Introduction:** This policy is about your obligations under the data protection legislation. Data protection is about regulating the way that the School uses and stores information about identifiable people (Personal Data). Data protection legislation also gives people various rights regarding their data - such as the right to access a copy of the Personal Data that the School holds on them. This policy documents our approach to personal data in accordance with UK Data Protection law, currently the Data Protection Act 2018 (GDPR) and other related legislation.

2 **Lawful treatment of data**: As a school, we will collect, store and process Personal Data about our staff, pupils, parents, suppliers and other third parties. We recognise that the correct and lawful treatment of this information will maintain confidence in the School and will ensure that the School operates successfully.

3 **Application**: This policy is aimed at all staff working in the School (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities, which includes employees, governors, self-employed teachers, contractors, agency staff, placement students and volunteers.

4 **Obligation**: You are obliged to comply with this policy when processing Personal Data on our behalf. Any breach of this policy may result in disciplinary action.

5 **Queries**: The Director of Finance and Operations (DFO) is responsible for helping you to comply with the School's obligations. All queries concerning data protection matters should be raised with the DFO.

What information falls within the scope of this policy

6 **Data Protection:** Data protection concerns information about individuals.

7 **Personal** Data: Personal Data is data which relates to a living person who can be identified either from that data, or from the other information that is available. Information as simple as someone's name and address is their Personal Data.

8 **Personal Data at work:** In order for you to do your job, you will need to use and create Personal Data. Virtually anything might include Personal Data.

9 Examples of places where Personal Data might be found are:

9.1 on a computer database;

9.2 in a file, such as a pupil report;

9.3 in a register or contract of employment;

9.4 pupils' exercise books, coursework and mark books;

9.5 health records; and

9.6 email correspondence.

10 Examples of documents where Personal Data might be found are:

10.1 a report about a child protection incident;

10.2 a record about disciplinary action taken against a member of staff;

10.3 photographs of pupils;

10.4 a tape recording of a job interview or disciplinary hearing;

10.5 contact details and other personal data held about pupils, parents and staff and their families;

10.6 contact details of a member of the public who is enquiring about placing their child at the School;

10.7 financial records of a parent;

10.8 information on a pupil's performance; and

10.9 an opinion about a parent or colleague in an email.

These are just examples - there may be many other things that you use and create that would be considered Personal Data.

11 **Special Categories of Personal Data:** The following categories are referred to as **Special Categories of Personal Data** in this policy. You must be particularly careful when dealing with Personal Data which falls into any of the categories below:

11.1 information concerning child protection matters;

11.2 information about serious or confidential medical conditions and information about special educational needs;

11.3 information concerning serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved);

11.4 financial information (for example about parents and staff);

11.5 information about an individual's racial or ethnic origin;

11.6 political opinions;

11.7 religious beliefs or other beliefs of a similar nature;

11.8 trade union membership;

11.9 physical or mental health or condition;

11.10 sex life or sexual orientation;

11.11 genetic information;

11.12 information relating to actual or alleged criminal activity; and

11.13 biometric information (e.g. a pupil's fingerprints following a criminal investigation).

If you have any questions about your processing of these Special Categories of Personal Data please speak to The Head or Headteacher.

Your obligations

12 **Personal Data must be processed fairly, lawfully and transparently.**

12.1 What does this mean in practice?

12.1.1 "Processing" covers virtually everything which is done in relation to Personal Data, including using, disclosing, copying and storing Personal Data.

12.1.2 People must be told what data is collected about them, what it is used for, and who it might be shared with, unless it is obvious. They must also be given other information, such as, what rights they have in their information, how long we keep it for and about their right to complain to the Information Commissioner's Office (the data protection regulator).

12.2 This information is often provided in a document known as a Privacy Notice. Copies of the School's Privacy Notices can be accessed on the School's website. You must familiarise yourself with the School's Pupil, Parent and Staff Privacy notices.

12.3 If you are using Personal Data in a way which you think an individual might think is unfair please speak to the Compliance Officer in the first instance.

13 **You must only process Personal Data for the following purposes:**

13.1 ensuring that the School provides a safe and secure environment;

13.2 providing pastoral care;

13.3 providing education and learning for our pupils;

13.4 providing additional activities for pupils and parents (for example activity clubs);

13.5 protecting and promoting the School's interests and objectives (for example fundraising);

13.6 safeguarding and promoting the welfare of our pupils; and

13.7 to fulfil the School's contractual and other legal obligations.

14 **Use of Personal Data:** If you want to do something with Personal Data that is not on the above list, or is not set out in the relevant privacy notice(s), you must speak to the DFO. This is to make sure that the School has a lawful reason for using the Personal Data. Please refer to Appendix 4 for details of the Data Protection Principles.

15 **Consent**: We may sometimes rely on the consent of the individual to use their Personal Data. This consent must meet certain requirements and therefore you should speak to the Compliance Officer if you think that you may need to obtain consent. If you are not an employee of the School (for example, if you are a volunteer), then you must be extra careful to make sure that you are only using personal information in a way that has been expressly authorised by the School.

16 **You must only process Personal Data for specified, explicit and legitimate purposes.**

16.1 What does this mean in practice?

16.1.1 For example, if pupils are told that they will be photographed to enable staff to recognise them when writing references, you should not use those photographs for another purpose (e.g. in the School's prospectus). Please see the School's Code of Conduct and the guidance for staff on the use of photographs and videos of pupils by the School for further information relating to the use of photographs and videos.

17 **Personal Data held must be adequate and relevant for the purpose.**

17.1 What does this mean in practice?

17.1.1 This means not making decisions based on incomplete data. For example, when writing reports you must make sure that you are using all of the relevant information about the pupil.

18 **You must not hold excessive or unnecessary Personal Data.**

18.1 What does this mean in practice?

18.1.1 Personal Data must not be processed in a way that is excessive or unnecessary. For example, you should only collect information about a pupil's siblings if that Personal Data has some relevance, such as allowing the School to determine if a sibling fee discount is applicable.

19 **The Personal Data that you hold must be accurate**.

19.1 What does this mean in practice?

19.1.1 You must ensure that Personal Data is complete and kept up to date. For example, if a parent notifies you that their contact details have changed, you should update the School's information management system.

20 **You must not keep Personal Data longer than necessary**.

20.1 What does this this mean in practice?

20.1.1 The School, Information and Record Retention policy has details about how long different types of data should be kept for and when data should be destroyed. This applies to both paper and electronic documents. You must be particularly careful when you are deleting data.

20.1.2 Please speak to the Compliance Officer for guidance on the retention periods and secure deletion.

21 **You must keep Personal Data secure**.

21.1 You must comply with the following School policies and guidance relating to the handling of Personal Data:

21.1.1 Data Protection policy

21.1.2 Taking Storing and Using Images of Pupils Policy;

21.1.3 ICT acceptable use policy for Staff; and

21.1.4 Information and records retention policy.

22 **You must not transfer Personal Data outside the EEA without adequate protection.**

22.1 What does this mean in practice?

22.1.1 If you need to transfer personal data outside the EEA please contact the Compliance Officer. For example, if you are arranging a school trip to a country outside the EEA.

N.B. This section is subject to change due to the BREXIT deal. It will be reviewed once further details are known.

Sharing Personal Data outside the School - dos and don'ts

23 Dos and don'ts: Please review the following dos and don'ts:

23.1 **DO** encrypt emails which contain Special Categories of Personal Data described in paragraph 11 above. For example, encryption should be used when sending details of a safeguarding incident to social services.

23.2 **DO** make sure that you have permission from your line manager to share Personal Data on the School website.

23.3 **DO** be aware of "blagging". This is the use of deceit to obtain Personal Data from people or organisations. You should seek advice from the ICT Manager where you are suspicious as to why the information is being requested or if you are unsure of the identity of the requester (e.g. if a request has come from a parent but using a different email address).

23.4 **DO** be aware of phishing. Phishing is a way of making something (such as an email or a letter) appear as if it has come from a trusted source. This is a method used by fraudsters to access valuable personal details, such as usernames and passwords. Don't reply to email, text, or pop-up messages that ask for personal or financial information or click on any links in an email from someone that you don't recognise. Report all concerns about phishing to the IT department.

23.5 **DO NOT** disclose Personal Data to the police without permission from the DFO (unless it is an emergency).

23.6 **DO NOT** disclose Personal Data to contractors without permission from the DFO. This includes, for example, sharing Personal Information with an external marketing team to carry out a pupil recruitment event.

Accessing or Sharing Personal Data within the School

24 **Sharing Personal Data:** This section applies when Personal Data is accessed or shared within the School. It also applies when Personal Data is shared between Redmaids' High and the Governing Body.

25 **Need to know basis**: Personal Data must only be accessed or shared within the School on a "need to know" basis.

Examples which are **likely** to comply with data protection legislation:

25.1 a teacher discussing a pupil's academic progress with other members of staff (for example, to ask for advice on how best to support the pupil);

25.2 informing an exam invigilator that a particular pupil suffers from panic attacks; and

25.3 disclosing details of a teaching assistant's allergy to bee stings to colleagues so that you / they will know how to respond (but more private health matters must be kept confidential).

Examples which are **unlikely** to comply with data protection legislation:

25.4 the Head/Headteacher being given access to all records kept by nurses working within the School (seniority does not necessarily mean a right of access);

25.5 a member of staff looking at a colleague's HR records without good reason. For example, if they are being nosey or suspect their colleague earns more than they do. In fact accessing records without good reason can be a criminal offence.

25.6 disclosing personal contact details for a member of staff (e.g. their home address and telephone number) to other members of staff (unless the member of staff has given permission or it is an emergency).

26 **Sharing of Personal Data and safeguarding:** You may share Personal Data to avoid harm, for example in child protection and safeguarding matters. You should have received training on when to share information regarding welfare and safeguarding issues. If you have not received this training please contact the Designated Safeguarding Lead (DSL) as a matter of urgency.

Individuals' rights in their Personal Data

27 **Rights**: People have various rights in their data. You must be able to recognise when someone is exercising their rights so that you can refer the matter to the DFO. These rights can be exercised either in writing (e.g. in an email) or orally.

28 **Individual's rights:** Please let the DFO know if anyone (either for themselves or on behalf of another person, such as their child):

28.1 wants to know what data the School holds about them or their child as this is a subject access request (see paragraph 30);

28.2 asks to withdraw any consent that they have given to use their data or data about their child;

28.3 wants the School to delete any data;

28.4 asks the School to correct or change information (unless this is a routine updating of information such as contact details);

28.5 asks for personal data to be transferred to them or to another organisation;

28.6 wants the School to stop using their information for direct marketing purposes. Direct marketing has a broad meaning for data protection purposes and might include communications such as the School newsletter or alumni events information; or

28.7 objects to how the School is using their data or wants the School to stop using their data in a particular way, for example, if they are not happy that data has been shared with a third party.

29 Please note, a person may be committing a criminal offence if they alter, block, erase, destroy or conceal information to prevent it from being disclosed (for example, to prevent its disclosure if a subject access request for that information has been received). Therefore if you are asked to provide data or documents to a colleague at the School who is preparing a response to a request for information then you must make sure that you provide everything.

Requests for Personal Data (Subject Access Requests)

30 **The right to request Personal Data:** One of the most commonly exercised rights mentioned in paragraph 32 **Error! Reference source not found.**below is the right to make a Subject Access Request. Under this right people are entitled to request a copy of the Personal Information which the School holds about them (or in some cases their child) and to certain supplemental information.

31 **Form of request:** Subject Access Requests do not have to be labelled as such and do not even have to mention data protection. For example, an email which simply states "Please send me copies of all emails you hold about me" is a valid Subject Access Request. You must always immediately let the DFO and Compliance Officer know when you receive any such requests.

32 **If you receive a Subject Access Request**: Receiving a Subject Access Request is a serious matter for the School and involves complex legal rights. Staff must never respond to a subject access request themselves unless authorised to do so. You must contact the DFO or the Compliance Officer.

33 **Disclosure**: When a Subject Access Request is made, the School must disclose all of that person's Personal Data to them which falls within the scope of the request - there are only very limited exceptions. There is no exemption for embarrassing information - so think carefully when writing letters and emails as they could be disclosed following a Subject Access Request. However, this should not deter you from recording and passing on information where this is appropriate to fulfil your professional duties, particularly in relation to safeguarding matters.

Breach

34 **Breach:** A breach of this policy may be treated as misconduct and could result in disciplinary action including in serious cases, dismissal.

35 **Criminal offence:** A member of staff who deliberately or recklessly obtains or discloses Personal Data held by the School without proper authority is also guilty of a criminal offence.

Appendix 1 – Procedures for Responding to Subject Access Requests

Redmaids' High School

This Appendix outlines our procedures for responding to subject access requests made under the Data Protection Act 2018.

Preservation of records

Redmaids' High School has produced an Information and Records Retention Policy which documents our retention policy for all key information.

This policy can be accessed here:

https://www.redmaidshigh.co.uk/about-us-school-policies.aspx

Rights of access to Data

There are two distinct rights of access to data held by schools about pupils.

1. Under the Data Protection Act 2018 any individual has the right to make a request to access the personal data held about them.

2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (England) Regulations 2005.

The following procedures relate to subject access requests made under the Data Protection Act 2018.

Actioning a subject access request (SAR)

1. Requests for data from staff, students and others must be made in writing; which includes email, and be addressed to the Head/Headteacher. If the initial request does not clearly identify the information required, then further enquiries will be made. The School will undertake a reasonable search for the requested information.

2. The identity of the requestor must be established before the disclosure of any data, and checks should also be carried out regarding proof of relationship if a child is involved. Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address

- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

This list is not exhaustive.

3. Any individual has the right of access to data held about them. However, with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Head/Headteacher should discuss the request with the child and take their views into account when making a decision. Where a request is made by an individual with parental responsibility, a child with competency to understand can refuse to consent to the request for their records. This is subject to the perceived level of maturity of the child. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the subject access request on behalf of the child.

4. The school may make a charge for the provision of data, dependent upon the following:
    - Should the data requested contain the educational record then the amount charged will be dependent upon the number of pages provided.
    - Should the data requested be personal data that does not include any data contained within educational records schools can charge up to £10 to provide it. The school reserves the right to charge an additional fee for multiple copies of data or multiple requests.
    - If the data requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the data can be made by the Head/Headteacher.

5. The response time for subject access requests, once officially received, is one calendar month. 'Day one' is the day of receipt, for example, a SAR received on 3 September should now be responded to by 3 October. **(During the school holidays, the SAR will be acknowledged but may require an extension to fulfill)**. However, the calendar month will not commence until after receipt of fees or clarification of data sought.

The Data Protection Act 2018 allows exemptions as to the provision of some data; **therefore, all data will be reviewed prior to disclosure**.

1. Third party data is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party data, consent should normally be obtained. There is still a need to adhere to the calendar month statutory timescale.

2. Any data which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should data that would reveal that the child is at risk of abuse, or data relating to court proceedings. Depending on the circumstances, the School might decide to not disclose some information based on other exemptions described in the Data Protection Act. More information on this, can be obtained from the ICO.

3. If there are concerns over the disclosure of data, then additional advice should be sought.

4. Where redaction (data blacked out/removed) has taken place then a full copy of the data provided should be retained in order to establish, if a complaint is made, what was redacted and why.

5. Data disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If data contained within the disclosure is difficult to read or illegible, then it should be retyped. The data does not have to be in the form of the original document and can be transferred to a separate document for ease of use. There is no requirement to translate the data into another language.

6. Data can be provided at the school with a member of staff on hand to help and explain matters if requested or provided at face-to-face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used, then registered/recorded mail must be used. If the data is sent via email the document must be password protected or encrypted.

Complaints

Complaints about the above procedures should be made to the Chair of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure. Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure data.

Contacts

If you have any queries or concerns regarding these policies and/or procedures referenced in this Policy then please contact the School's Compliance Officer directly at privacy@redmaidshigh.co.uk. Further advice and information can also

be obtained from the Information Commissioner's Office, www.ico.gov.uk or telephone 0303 123 1113.

Appendix 2

Data Protection Codes of Practice for Staff

a) When writing minutes, memoranda, sending notes or letters, or sending e-mails the composer must think about the level of confidentiality involved and question whether the proposed method of communication is appropriate. The names of pupils, colleagues or parents are never used in the 'subject field' of an email; a generic title must be used instead e.g. Yr 11 student. Care must be taken to ensure files are saved correctly and confidential material is password protected if appropriate.

b) Strictly confidential material should be placed in an envelope, marked "Strictly Confidential", and given to the Head's Personal Assistant or the Headteacher. This should remain sealed, except when in use. The Head/Headteacher should decide when this material should be accessed and by whom.

c) Important interviews with students about discipline problems or other concerns must be recorded, dated and signed. If a very sensitive issue is involved the student must be warned beforehand that what she says will be treated in confidence, but that another adult (staff or outside agency) may have to be called in.

d) Important interviews with parents/guardians about discipline problems or other concerns must be recorded, dated and signed. If a very sensitive issue is involved the parent or guardian must be warned that what they say will be treated in confidence, but that another member of staff or an outside agency may have to be called in.

e) Staff who are not directly involved in a medium to strictly confidential matter will only be told about it on a need-to-know basis.

f) The Management Information System (SIMS) database can be accessed by all academic staff and administrative staff where necessary for their role. The levels of access are determined by staff roles and responsibilities. A few members of the office staff and academic staff with executive curriculum responsibility are enabled to make changes as set out within their job descriptions.

g) The Financial database is accessible to Bursary staff only.

h) The Admissions database is accessible to Admissions and some Marketing staff and some Senior Management only.

i) No member of staff should give out personal data concerning any other member of staff or their family, or any pupil and her family (including telephone numbers), without first requesting permission to do so.

j) No member of staff should access personal records for their own purpose, for example, looking at their daughter's SIMs record.

k) All staff must adhere to the ICT Staff Acceptable Use Agreement and not share passwords.

l) It is essential that all staff lock their PC or iPads when they are not at their desk.

m) Information concerning staff appointments and applications is strictly confidential to the people to whom it is delegated. All documentation is shredded or held by the Head/Headteacher post interview.

n) No document which mentions a third party may be seen by the subject of the documentation. If a document refers to person x and also to person y, x cannot see the document unless person y's identity is removed. Other documents concerning staff or students may be seen by the person / people to whom it / they relate upon request, providing a check with the third party has been carried out by the Head/Headteacher or her delegated representative, or details of the identity removed.

o) The alumnae system, hosted by Potentiality, is only accessed by the Development and Alumnae Officers. Resultant donor communications, donation logs and analysis work (mail merges, excel spreadsheets etc) are accessed by Marketing and Development.

p) The safeguarding recording system, CPOMS, can be accessed by staff and administrative staff where necessary for their role. The levels of access are determined by staff roles and responsibilities.

q) Staff must contact the Head of IT and Compliance Officer if they wish to use a new system or software that stores personal data. This is so that all due diligence can be done in accordance with Article 30 of the GDPR. In some cases a Data Processing Impact Assessment (DPIA) will need to be completed prior to using the system.

Processing of visual images

Visual images in the form of photos, videos or other means are very often taken, recorded, used and sometimes retained in relation to school activities whether academic or otherwise.

Redmaids' High's approach to this is covered in two separate policies:

- CCTV and Minibus Dashboard Camera Policy
- Taking, Storing and Using Images of Pupils Policy

Both of these can be accessed here:

https://www.redmaidshigh.co.uk/about-us-school-policies.aspx

Accessing school data remotely – Data Access

All staff are bound by the school's Staff ICT Acceptable Use Policy Agreement, revised to support GDPR compliance.

It can be accessed here: https://www.redmaidshigh.co.uk/about-us-school-policies.aspx

School data can be accessed remotely via Foldr, Secure Portal, The Hub or One Drive. These access points are provided only for use of staff and students of the school. This confidential data, including photographs of students, must not be stored on any personal device in accordance with the Staff ICT Acceptable Use Policy Agreement and the school's Guide to Safer Working Practice; Behaviour and Code of Conduct.

Access is granted only on condition that the individual formally agrees to the terms of this Policy.

Personal use

Data made available through the remote access is confidential and protected by law under the Data Protection Act 2018.

Users must not distribute or disclose any data obtained from remote school access to any person(s) with the exception of the student to which the data relates or to other adults with parental responsibility.

Users should not attempt to access the network in any environment where the security of the data may be placed at risk.

Parental Access to student data via the Hub

Parental access to school data via the Hub is via a secure protocol which can only be granted by using the details provided by the school. **Users must assume personal responsibility for their passwords.**

Questions, Complaints and Appeals

Hub users should address any concerns and enquiries to the Head/Headteacher.

Redmaids' High School reserves the right to revoke or deny access to the Hub of any individual under the following circumstances:

- The validity of parental responsibility is questioned
- Court ruling preventing access to child or family members is issued
- Users found to be in breach of the Hub usage policy

If any Child Protection concerns are raised or disputes occur the school will revoke access for all parties concerned pending investigation. Users are liable for any potential misuse of the system and/or breach of the Data Protection Act 2018 that may occur as a result of failing to adhere to any of the rules/guidelines listed in this document.

Please note: where the Hub access is not available, Redmaids' High School will still make data available according to Data Protection Act law.

Appendix 3 - A Guide to Confidentiality

Data gathered and kept within the school may be divided into five types:

A. Very low in confidentiality: access by any academic staff member; the student or her parent/guardian by arrangement.

- Termly Progress Reports re Standard of Work and Attitude
- Copies of students' annual full reports and progress reports
- Copies of personal assessment documentation e.g. targets
- Marks/examination results (internal & external)
- Records of order marks / detentions/ blue slips.

B. Low in confidentiality: access by any academic member of staff; the tutor; the student or her parent/guardian by arrangement.

- Records of entry examinations and interviews
- Baseline Test results
- Short Reports
- Data supplied by feeder schools
- Addresses and telephone numbers of separated parents/guardians
- Enquiries about entry to the school
- Data concerning individual students: Statements of Special Educational Needs, Learning Difficulties and Disabilities and English as a Foreign Language.

C. Mid-range confidentiality: access by Heads of Department, Heads of Year and others by delegation; the student or her parent /guardian by arrangement.

- Memoranda about any concerns (e.g. bullying)
- Incident forms
- Minutes of Departmental or Pastoral meetings.

D. Strictly confidential: access by the Head / Headteacher/Chief Operating Officer/ others by delegation.

- Copies of UCAS applications (also Director/Head of Sixth Form)
- References written for students / other schools
- Personal circumstances around the reasons for parents/guardians separatingData about assisted places / bursaries
- Sensitive data about which student, parent/guardian or staff ask for strictest confidentiality
- Data concerning abuse – matters covered by the Children's Act
- Staff records
- Data about parents'/guardians' financial applications

E. Medical confidentiality: access by the School Nurse/ Head/ Headteacher/First Aid others by delegation e.g. parents, students, pastoral heads etc. on a 'need to know' basis only.

- Medical Records
- Data re medical conditions

N.B. Health professionals are bound by the medical code of confidentiality in their work.

3. Outside Agencies

Where outside agencies and others provide support for the PSHE and citizenship provision, they must be made aware of, and abide by, the school's policies for PSHE, including disclosures and confidentiality. However, they may also have a role in providing advice and support directly to young people. The boundary between these two roles must be agreed with the school. Students must be clear about what their rights to confidentiality are.

All teaching staff should be aware of the school's guidelines on letter writing, about when and how communications should be sent to parents/guardians. In the cases of letters and replies, staff should examine the above list to ensure the correct degree of confidentiality.

Appendix 4 - Data Protection Principles – Data Protection Act 2018

The Data Protection Act 2018 establishes six enforceable principles that must be adhered to at all times:

1. First data protection principle – processing must be lawful and fair;
2. Second data protection principle – purposes of processing must be specified, explicit and legitimate;
3. Third data protection principle; personal data must be adequate, relevant and not excessive;
4. Fourth data protection principle; personal data must be accurate and kept up to date;
5. Fifth data protection principle; personal data must be kept for no longer than is necessary;
6. Sixth data protection principle; personal data must be processed in a secure manner; and;
7. Seventh data protection principle; the data controller has accountability for their actions and responsibility for monitoring how compliance is achieved.

Linked documents:

Privacy Notice for Parents
Privacy Notice for Older Pupils
Privacy Notice for Younger Pupils
Privacy Notice for Staff
Privacy Notice for Alumnae, Relations, Development and Fundraising
Privacy Notice for Visitors
CCTV and Dashboard Camera Policy
Taking, Storing and Using Images Policy
Information and Records Retention Policy
Data Breach Policy
Direct Marketing Policy
Website Privacy and Cookie Policy
Staff ICT Acceptable Use Policy Agreement
Redmaids' High School Guide to Safer Working Practice; Behaviour and Code of Conduct for Staff

Reviewed and updated Kate Doarks/S Bramley-Dymond/L Brown/Paul Dwyer/Richard Bacon Reviewed April 2021

Review date April 2022