REDLAND GREEN SCHOOL
BRISTOL

DATA PROTECTION & PERSONAL DATA HANDLING POLICY

1 POLICY AIMS

1.1 Redland Green School's Data Protection & Personal Data Handling Policy sets out the school's commitment to protecting personal data and how the school implements that commitment with regards to the collection and use of personal data. Redland Green School is committed to:

i) Ensuring that the school complies with the eight data protection principles, as listed below

ii) Meeting the legal obligations as laid down by the Data Protection Act 1998

iii) Ensuring that data is collected and used fairly and lawfully

iv) Processing personal data only in order to meet the school's operational needs or fulfil legal requirements

v) Taking steps to ensure that personal data is up to date and accurate

vi) Establishing appropriate retention periods for personal data

vii) Ensuring that data subjects' rights can be appropriately exercised

viii) Providing adequate security measures to protect personal data so that it cannot be accessed by anyone who does not have permission to access that data and/or needs to have access to that data

ix) Ensuring that a nominated officer is responsible for data protection compliance and provides a point of contact for all data protection issues

x) Ensuring that all staff are made aware of good practice in data protection

xi) Providing adequate training for all staff responsible for personal data

xii) Ensuring that everyone handling personal data knows where to find further guidance

xiii) Ensuring that queries about data protection, internal and external to the school, is dealt with effectively and promptly

xiv) Regularly reviewing data protection procedures and guidelines within the school

2 DATA PROTECTION PRINCIPLES

2.1 The eight data protection principles are:

1) All personal data will be fairly obtained in accordance with the 'Privacy Notice' and lawfully processed in accordance with the 'Conditions for Processing'.

2) Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3) Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4) Personal data shall be accurate and, where necessary, kept up to date.

5) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6) Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998.

7) Appropriate technical and organisational measures shall be taken against unauthorised and unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8) Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

3 CONDITIONS FOR PROCESSING

3.1 The conditions for processing are set out in Schedules 2 and 3 to the Data Protection Act. Unless a relevant exemption applies, at least one of the following conditions must be met whenever personal data is processed:

1) The individual who the personal data is about has consented to the processing

2) The processing is necessary:

   i) In relation to a contract which the individual has entered into; or

   ii) Because the individual has asked for something to be done so they can enter into a contract

3) The processing is necessary because of a legal obligation that applies to the school (except an obligation imposed by a contract)

4) The processing is necessary to protect the individual's 'vital interests'. This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's Accident & Emergency Department treating them after a serious accident

5) The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions

6) The processing is in accordance with the 'legitimate interests' condition

3.2 WHAT IS THE 'LEGITIMATE INTERESTS' CONDITION?

The Data Protection Act recognises that people may have legitimate reasons for processing personal data that the other conditions for processing do not specifically deal with. The 'legitimate interests' condition is intended to permit such processing, provided it meets certain requirements.

3.3 The first requirement is that the data handler must need to process the information for the purposes of their legitimate interests or for those of a third party to whom it is disclosed.

3.4 The second requirement, once the first has been established, is that these interests must be balanced against the interests of the individual(s) concerned. The 'legitimate interests' condition will not be met if the processing is unwarranted because of its prejudicial effect on the rights and freedoms, or legitimate interests, of the individual. The data handler's legitimate interests do not need to be in harmony with those of the individual for the condition to be met. However, where there is a serious mismatch between competing interests, the individual's legitimate interests will come first.

3.5 Finally, the processing of information under the legitimate interests condition must be fair and lawful and must comply with all the data protection principles.

3.6 **WHAT CONDITIONS NEED TO BE MET IN RESPECT OF SENSITIVE PERSONAL DATA?**

At least one of the conditions must be met whenever personal data is processed. However, if the information is sensitive personal data, at least one of several other conditions must also be met before the processing can comply with the first data protection principle. These other conditions are as follows:

1) The individual who the sensitive personal data is about has given explicit consent to the processing

2) The processing is necessary so that the data handler can comply with employment law

3) The processing is necessary to protect the vital interests of:

4) The individual (in a case where the individual's consent cannot be given or reasonably obtained), or

5) Another data handler (in a case where the individual's consent has been unreasonably withheld)

6) The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. Extra limitations apply to this condition

7) The individual has deliberately made the information public

8) The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights

9) The processing is necessary for administering justice, or for exercising statutory or governmental functions

10) The processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality

11) The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals

3.7 In addition to the above conditions – which are all set out in the Data Protection Act itself – regulations set out several other conditions for processing sensitive personal data. Their effect is to permit the processing of sensitive personal data for a range of other purposes – typically those that are in the substantial public interest, and which must necessarily be carried out without the explicit consent of the individual. Examples of such purposes include preventing or detecting crime and protecting the public against malpractice or maladministration. A full list of the additional conditions for processing is set out in the Data Protection (Processing of Sensitive Personal Data) Order 2000 and subsequent orders.

3.8 **WHEN IS PROCESSING 'NECESSARY'?**

Many of the conditions for processing depend on the processing being 'necessary' for the particular purpose to which the condition relates. This imposes a strict requirement, because the condition will not be met if the organisation can achieve the purpose by some other reasonable means or if the processing is necessary only because the organisation has decided to operate its business in a particular way.

3.9 **WHAT IS MEANT BY 'CONSENT'?**

One of the conditions for processing is that the individual has consented to their personal data being collected and used in the manner and for the purposes in question.

3.10 The data handler will need to examine the circumstances of each case to decide whether consent has been given. In some cases this will be obvious, but in others the particular circumstances will need to be examined closely to decide whether they amount to an adequate consent.

3.11 Consent is not defined in the Data Protection Act. However, the European Data Protection Directive (to which the Act gives effect) defines an individual's consent as:

"…any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".

3.12 The fact that an individual must 'signify' their agreement means that there must be some active communication between the parties. An individual may 'signify' agreement other than in writing, but organisations should not infer consent if an individual does not respond to a communication – for example, from a parent's failure to return a form or respond to a leaflet.

3.13 Consent must also be appropriate to the age and capacity of the individual and to the particular circumstances of the case. For example, if the school intends to continue to hold or use personal data after the relationship with the individual ends, then the consent should cover this. Even when consent has been given, it will not necessarily last forever. Although in most cases consent will last for as long as the processing to which it relates continues, the data handler should recognise that the individual may be able to withdraw consent, depending on the nature of the consent given and the circumstances in which the data handler is collecting or using the information. Withdrawing consent does not affect the validity of anything already done on the understanding that consent had been given.

3.14 The data handler should review whether a consent he/she has been given remains adequate as the school's relationship with an individual develops, or as the individual's circumstances change.

3.15 Consent obtained under duress or on the basis of misleading information does not adequately satisfy the condition for processing.

3.16 The Data Protection Act distinguishes between:

1) The nature of the consent required to satisfy the first condition for processing; and

2) The nature of the consent required to satisfy the condition for processing sensitive personal data, which must be 'explicit'

4 DATA BREACHES

4.1 Data breaches can have serious effects on individuals and/or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

4.2 Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance.

5 PERSONAL DATA

5.1 The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

i) Personal information about members of the school community including pupils, members of staff and parents/carers eg names, addresses, contact details, legal guardianship contact details, health records, disciplinary records

ii) Curricular/academic data eg class lists, pupil progress records, reports, references

iii) Professional records eg employment history, taxation and national insurance records, appraisal records and references

iv) Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members

6 REGISTRATION

6.1 The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

7 INFORMATION TO PARENTS – THE 'PRIVACY NOTICE'

7.1 In order to comply with the fair processing requirements of the Data Protection Act (DPA), the school will inform parents of all students of the data they collect, process and hold on the students, the purposes for which the data is held and the third parties (eg Local Authority (LA), Department for Education (DfE), etc) to whom it may be passed. This privacy notice will be passed to parents using the school's website and is also included as Appendix 1 of this policy.

8 RISK ASSESSMENT

8.1 Information risk assessments will be carried out by Data Protection Nominated Officer to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

i) Recognizing the risks that are present

ii) Judging the level of the risks (both the likelihood and consequences)

iii) Prioritising the risks

9 SECURE STORAGE OF & ACCESS TO DATA

9.1 The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

9.2 All users will use strong passwords which must be changed regularly. User passwords must never be shared.

9.3 Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

9.4 All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

9.5 Personal data can only be stored on school equipment (this includes computers and portable storage media. Private equipment (ie owned by the users) must not be used for the storage of personal data.

9.6 When personal data is stored on any portable computer system, USB stick or any other removable media:

i) The data must be encrypted and password protected

ii) The device must be password protected where possible (it is recognised that some memory sticks/cards and other mobile devices cannot be password protected)

iii) The device must offer approved virus and malware checking software where possible (it is recognised that memory sticks will not provide this facility and most mobile devices will not offer malware protection)

iv) The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

9.7 The school has a clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups; all paper based protected and restricted material must be held in lockable storage.

9.8 The school recognises that under Section 7 of the DPA data subjects have a number of rights in connection with their personal data, the main one being the right of access. Any requests to see all or a part of the personal data held by the school should be submitted in writing for the attention of the Headteacher. Data subjects have the right to know if the school holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification, blocking, erasure and destruction of data.

10 SECURE TRANSFER OF DATA & ACCESS OUT OF SCHOOL

10.1 The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

i) Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location

ii) Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school

iii) When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform

iv) If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location

v) Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software

vi) Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the LA (if relevant) in this event

11 DISPOSAL OF DATA

11.1 The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

11.2 The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated or otherwise disintegrated for data. A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

12 AUDIT LOGGING, REPORTING & INCIDENT HANDLING

12.1 An audit log will be kept to provide evidence of accidental or deliberate data security breaches including loss of protected data or breaches of the Staff, Governor & Volunteer ICT Acceptable Use Policy Agreement, for example.

12.2 The school's policy for reporting, managing and recovering from information risk incidents, establishes:

i) A 'responsible person' for each incident

ii) A communications plan, including escalation procedures which results in a plan of action for rapid resolution

iii) A plan of action of non-recurrence and further awareness raising

12.3 All significant data protection incidents must be reported through the Data Protection Nominated Officer to the Information Commissioner's Office.

13 REFERENCES

13.1 The Governing Body shall request (*open/closed*) references and shall provide (*open/closed*) references except where an employee has specifically requested that a (*open/closed*) reference be supplied.

13.2 Referees will be advised that the Governing Body has a (*open/closed*) policy on references.

13.3 The Governing Body will comply with DfE guidance on references as issued from time to time in particular in relation to safeguarding children and safer recruitment in education.

14 RETENTION OF PERSONAL DATA FOR STAFF

14.1 Personal data for staff will be held only for clearly specified purposes as indicated in Appendix 2.

15 TRAINING

15.1 All new and existing employees who handle personal information will receive training on data protection procedures, which includes information about the standards the school expects its employees to observe in the use of personal information.

16 LINKS WITH OTHER POLICIES

16.1 This policy has links with the following school policies:

- Confidentiality Policy
- Freedom of Information Policy
- Governors' Code of Conduct Policy
- Safeguarding & Child Protection Policy
- Whistle-blowing Policy

Agreed by Staff	Agreed by Pupils	Agreed by Governors	Review Schedule	Date Reviewed	Date Reviewed	Date Reviewed	Date Reviewed
N/A	N/A	25 MAR 2014	2 YEARS	06 NOV 2014	12 NOV 2015		
Date Reviewed	Date Reviewed	Date Reviewed	Date Reviewed	Date Reviewed	Date Reviewed	Date Reviewed	Date Reviewed

APPENDIX 1 – PRIVACY NOTICE

PRIVACY NOTICE – DATA PROTECTION ACT 1998

Redland Green School is a Data Controller for the purposes of the Data Protection Act. The school collects information from parents/carers and may receive information about pupils and families from the child's previous school and the Learning Records Service. The school holds this personal data and uses it to:

- Support pupils' teaching and learning
- Monitors and reports on pupil progress
- Provides appropriate pastoral care
- Assesses how well the school is doing

This information includes contact details, National Curriculum assessment results, attendance information and personal characteristics such as a child's ethnic group, any special educational needs (SEN) and relevant medical information.

The school will not give information about a child or family to anyone outside the school without consent unless the law and the school rules allow it to.

The school is required by law to pass some information about a child to the Local Authority (LA) and the Department for Education (DfE).

If you want to see a copy of the information about your child that the school holds and/or shares, please contact the school in writing addressed to the Headteacher.

If you require more information about how the LA and/or DfE store and use a child's information, then please go to the following websites:

http://www.bristol.gov.uk/page/council-and-democracy/data-protection-act

and

http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause

If you are unable to access these websites please contact the school.

APPENDIX 2 – RETENTION OF PERSONAL DATA FOR STAFF

This schedule lists the principal documents held on an employee's file. The list is not, however, exhaustive and other documents relating to employment may be held. Personnel files will be held for the length of employment + 7 years at which time they will be shredded. Documents relating to child protection or accidents at work may be held indefinitely. In this case the employee will be advised that this is the case. All of the documents held on the employee's file are held for the purpose of managing the employment relationship.

Document	Period of retention
Unsuccessful candidate Information	1 year from recruitment date
Original job application form	Termination + 7years
Two original references	Termination + 7years
Copy of contract of employment and any variation letters	Termination + 7years
Original contract acceptance	Termination + 7years
Confirmation of pre-employment medical check clearance	Termination + 7years
Confirmation of DBS clearance	Indefinitely
Barred list clearance	Indefinitely
Copies of documents used for identity authentication for DBS and Asylum & Immigration Act purposes	Termination + 7years
Copies of qualifications certificates relevant to employment	Termination + 7years
Formal disciplinary warnings – child protection related	Indefinitely
Formal disciplinary warnings – not child protection related	In accordance with the school's policy
Staff induction including NQTs Induction	Termination + 7years
UK Border Agency Documentation (Work permit)	Termination + 7 years
Letter of resignation and acceptance of resignation or other documentation relating to the termination of employment.	Termination + 7 years
Exit interview notes	Termination + 7 years
Salary assessment forms - teachers	Current year + 6 years
Time sheets	Current year + 6 years
Appraisal information	Current year + 6 years
NQT – satisfactory completion of skills tests.	Termination + 7years
Medical certificates and sickness absence record	Current year + 6 years
Other special leave of absence including parental leave, maternity leave	Current year + 6 years
Records relating to accident/injury at work	Termination + 7years. In the case of serious accidents a further retention period will need to be applied