Data Protection Policy

This policy was approved and ratified by the Governing Body of

Cox Green School

on 18 October 2016

Version	Authorisation	Approval Date	Effective Date	Next Review
1	Full Governing Body	Jan 14	Jan 14	Sept 14
1.1	Full Governing Body	21/10/14	21/10/14	Sept 15
1.3	Full Governing Body	20/10/15	20/10/15	Sept 2016
1.4	Full Governing Body	18/10/16	18/10/16	Oct 2018

Introduction

The Governing Body of the school has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.

The Headteacher and Governors of this School intend to comply fully with the requirements and principles of the Data Protection Act 1998. All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.

Enquiries

Information about the school's Data Protection Policy is available from the school office. General information about the Data Protection Act can be obtained from the Information Commissioner's Office (website www. ICO.gov.uk).

Data Protection Principles

All members of staff employed in our school are required to adhere to the eight data protection principles set out in the 1998 Data Protection Act:

1. Data shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner in compatible 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 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 Act.
7. Appropriate technical and organizational measures shall be taken against unauthorized or 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.

1 Fair Obtaining and Processing

Cox Green School undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data are held, the likely recipients of the data and the data subjects' right of access. Information about the use of personal data is printed on the appropriate collection form. If details are given verbally, the person collecting will explain the issues before obtaining the information.

> **"processing"** means obtaining, recording or holding the information or data or carrying out any or set of operations on the information or data.
>
> **"data subject"** means an individual who is the subject of personal data or the person to whom the information relates.

"personal data" means data, which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, Internet or media.

"parent" has the meaning given in the Education act 1996, and includes any person having parental responsibility or care of a child.

2. Registered Purposes

The Data Protection Registration entries for the School are available on the ICO website.
https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

The registration code for Cox Green is **Z2915512**

3. Data Integrity

The school undertakes to ensure data integrity by the following methods:

Data Accuracy - Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the School of a change of circumstances their computer record will be updated as soon as is practicable. A printout of their data record will be provided to data subjects every twelve months so they can check its accuracy and inform the school of any amendments required.

Where a data subject challenges the accuracy of their data, the School will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Governing Body for their judgement. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

Data Adequacy and Relevance -Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the School will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data. The MIS Administrator and Data Manager will review the data regularly and make recommendations to the Business Manager re adequacy and relevance.

Length of Time - Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the HR /Administrative Manager and the Business Manager to ensure that obsolete data are properly erased in line with the retention policy.

4. Subject Access

The Data Protection Act extends to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of

requests is in place. Where a request for subject access is received from a student, the school's policy is that:

- Requests from students will be processed as any subject access request as outlined below and the copy will be given directly to the student, unless it is clear that the student does not understand the nature of the request.

- Requests from students who do not appear to understand the nature of the request will be referred to their parents or carers.

- All children aged 12 and over have their own information rights provided they are Fraser competent (they are considered mature enough to understand the data). Any subject access request made from a parent of a child aged 12 and over will only be processed if the school have consent from the child to disclose the information to the parent and that the school are satisfied the consent was freely given.

- Parents have a right to a copy of their child's education record, regardless of the age of the child, until the child ceases to be in education.

Processing Subject Access Requests

Requests for access must be made in writing. In many cases a letter to the Headteacher will be sufficient to identify the information required. Alternatively, a Data Access form is provided in appendix 1.

Students, parents or staff may ask for a Data Access form, available from the School Office. Completed forms should be submitted to the Headteacher. Provided that there is sufficient information to process the request, a record will be made showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (eg Student Record, Personnel Record), and the planned date of supplying the information (normally not more than 40 calendar days from the request date). Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the request deadline will be 40 calendar days from the date of receipt of the additional information.

Requests from Carers who do not have parental responsibility will be considered by the Headteacher on an individual basis who will obtain legal advice if required on how to make a legal disclosure.

The Headteacher must be confident of the identity of the individual making the request. If not, this can be checked by the request to provide photographic ID such as passport or photo driving licence.

Note: In the case of any written request from a parent regarding their own child's record, access to the record will be provided within 15 school dates in accordance with the current Education (Pupil Information) Regulations.

The school may charge no more than £10 for a subject access request and £50 for an education record. The 40 calendar day deadline will start once the fee has been paid and any identify checks completed. The 40 calendar day provision applies only when school is open for business. When it is closed for school holidays the clock is stopped.

All files must be reviewed before any disclosure takes place. The data subject is only entitled to information about them. Any other individuals mentioned within the records must be redacted. The redaction may entail removal of information or anonymisation/pseudonymisation of the documents.

Where information has been provided to Cox Green School by a third party, for example, the local authority, the police, a health care professional or another school, but is held on the school's file it is normal to seek the consent of the third party before disclosing information. The 40 day timescale should be taken into account in this process. If the third party does not consent or consent is not explicitly given it may be necessary to seek additional advice.

The applicant should be told the data that the school holds, be given a copy of the data, and be told the purposes for which it is processed and whether it has been shared with any other party. It is good practice to explain whether data has been withheld and if so why. The Headteacher must at all times consider the welfare of the child.

Where particular data in a document cannot be disclosed a permanent copy should be made and the data obscured and re-copied. A full copy of the document before obscuring and the altered document should be retained together with the reason why the document was altered, so that in the event of a complaint there is an audit trail of what was done and why.

If the applicant wishes to complain they should write to the Chair of Governors and be given the details of the Information Commissioners Office.

5. Authorised Disclosures

The School will, in general, only disclose data about individuals with their consent. However there are circumstances under which the School's authorised officer may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- Student data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations.
- Student data disclosed to authorised recipients in respect of their child's health, safety and welfare.
- Student data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanor within or in the vicinity of the school, as per their right to receive a copy of their child's educational record.
- Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.
- Unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form committing not to disclose the data outside the school. Officers and personnel working on behalf of the local authority, are contractually bound not to disclose personal data.

- Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the school by administrative staff, teachers and other staff will only be made available where the person requesting the information is a professional legitimately working within the school who **need to know** the information in order to do their work. The school will not disclose anything on students' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything that suggests where they are, or have been, either the subject of or at risk of child abuse.

  A **"legal disclosure"** is the release of personal information from the computer to someone who requires the information to do his or her job within or for the school, provided that the purpose of that information has been registered.

  An **"illegal disclosure"** is the release of information to someone who does not need it, or has no right to it, or one which falls outside the School's registered purposes.

6. Data and Computer Security

Cox Green School undertakes to ensure security of personal data by the following general methods:

Physical Security

Appropriate building security measures are in place, such as alarms, window bars, deadlocks and computer hardware cable locks. Only authorised persons are allowed in the server room. Disks and printouts are locked away securely when not in use. Visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied.

Logical Security

Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up (i.e. security copies are taken) regularly. Any computers taken off-site are encrypted.

Procedural Security

In order to be given authorised access to the computer, staff will have to undergo checks and will sign a confidentiality agreement. All staff are trained in their Data Protection obligations and their knowledge updated as necessary.

Computer printouts as well as source documents are shredded before disposal.

Staff receive data protection training at induction regular update training.

Overall security policy for data is determined by the Governing Body and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent.

Any queries or concerns about security of data in the school should in the first instance be referred to the Business Manager.

Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

7. Advice

Additional advice for staff operating this procedure can be obtained from the Council's Data Protection Officer (dpa@rbwm.gov.uk). The fees for this service are published in the Services for Education and Local Authorities Traded Services Brochure.

8. Complaints

Complaints about the operation of these procedures should be made to the Chair of the Governing Body who will decide if it is appropriate for the complaint to be dealt with under the complaints procedure. Individuals who have exhausted the complaints procedure and remain unhappy should be directed to the Information Commissioners Office.

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
Tel: 0303 123 1113

https://ico.org.uk/

9. **Communication of policy**

This policy is published on the school website and the staff information drive. Staff are required to sign a confidentiality statement on appointment and training is provided.

10. **Evidence of implementation**

The Headteacher reports training, issues or breaches to the Governors Finance and Resources Committee.

11. Review of Policy

This policy shall be reviewed every 2 years by the Finance & Resources Committee.

Appendix A

ACCESS TO PERSONAL DATA REQUEST FORM

DATA PROTECTION ACT 1998 - Section 7

SURNAME	FORENAME
ADDRESS Postcode	Contact Telephone numbers: Home: Mobile:
Are you the person who is the subject of the records you are enquiring about (i.e. the "Data Subject")?	Yes / No *delete as appropriate
IF NO Are you a parent as defined by the Education Act 1996 of a child who is the "Data Subject" of the records you are enquiring about?	Yes / No *delete as appropriate
If YES, Name of child or children about whose personal data records you are enquiring	Child or children's names and dates of birth …… …… …… ……
Description of Concern/Area of Concern	
Description of Information or Topic(s) Requested	
Additional Information	

Please dispatch Reply to: *(if different from enquirer's details as stated on this form)*

Name
Address
Postcode

DATA SUBJECT DECLARATION

I request that the School search its records based on the information supplied above under Section 7 (1) of the Data Protection Act 1998 and provide a description of the personal data found from the information described in the details outlined above relating to me, (or my child/children), being processed by the School.

I agree that the reply period will commence when I have supplied sufficient information to enable the School to perform the search.

I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and Address above who I have authorised to receive such information).

Signature of "Data Subject" (or Subject's Parent) ……

Name of "Data Subject" (or Subject's Parent) (PRINTED) ……..

Dated ……..

Appendix B

Personal Device - School Email Agreement

Cox Green School expects employees to take responsibility in protecting the schools data as part of their role under the data protection act. This data includes all electronic communication such as email provided by the school. Staff have an obligation to ensure this data is safe and secure whether using a school issued device or otherwise. Some basic requirements that staff must agree to before being able to synchronise school email to their personal device are listed below.

1. The employee must ensure their personal device has at least basic password protection, this could be in the form of a pin number to unlock the device. The device must have the lock feature set to lock the device automatically within a reasonable time.
2. The employee should take reasonable precautions to prevent loss and theft of the device, this may include a tracking app or built in tracking service. The employee may wish to subscribe to services allowing the ability to remotely wipe all data from their device.
3. The employee must ensure no third party applications can access the data inside their emails while on their device. Applications such as chat applications and social media applications may scan contacts within the email application.
4. The employee must ensure no other persons can access their school email accounts via their personal device.
5. The employee's personal device can and will be wiped (remotely or otherwise) of all school related information if the device is reported lost or stolen and upon the termination of employment;
    i) The employee understands that this wiping could and most likely will result in the loss of personal data or information; and
    ii) The employee indemnifies the employer for any loss or damage that may result from the wiping of the device under this agreement.
6. School email accounts must be removed securely from any personal device upon termination.
7. Loss / Theft of a personal device that is linked to school email must be reported immediately to the IT Systems Manager.
8. The employee must remove their school email and securely wipe their personal device before attempting to dispose, sell, gift or other.
9. Cox Green School reserves the right to deny access to school email from personal devices at any time without warning.
10. The IT Support Department cannot provide any support for any personal devices, other than providing the standard connection information.
11. The employee must conform to all other school policies as per their employment contract, specifically in regards to IT, Social Media and Mobile Phone Use in relation to this agreement.
12. Please refer to the school's ICT Policy for all other enquires.

I understand and accept Cox Green School IT Department has the right to remotely wipe my device(s), I accept this and the terms listed above to have access to school email on my personal device(s).

Signed: _____ Date:_____