Data Protection Policy

This policy was approved and ratified by the Finance & Resources Committee of

Cox Green School

on 12th March 2024

Version	Authorisation	Approval Date	Effective Date	Next Review
V1	Governing Board	10/7/18	10/7/18	July 2020
V1.2	Finance & Resources Committee	28/4/20	28/4/20	April 2022
V1.3	Finance & Resources Committee	29/3/22	29/3/22	29/3/24
V1.4	Finance & Resources Committee	12/3/24	12/3/24	March 2026

Contents:

1. Statement of Intent

Cox Green School is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the Data Protection Act 2018 as set out in the Data Protection Bill.

The school may be required to share personal information about its staff or pupils with other organisations, mainly the Local Authority (LA), other schools and educational bodies, and other agencies such as social services.

This policy is in place to ensure all staff and Trustees are aware of their responsibilities and outlines how the school complies with the following core principles of the Data Protection Act 2018.

Organisational methods for keeping data secure are imperative, and Cox Green School believes that it is good practice to have clear practical policies.

This policy complies with the requirements set out in the Data Protection Act 2018, which took effect from 25 May 2018.

2. Legal Framework

2.1 This policy has due regard to legislation, including, but not limited to the following:

- The Data Protection Act 2018;
- The UK General Data Protection Regulation (UK GDPR);
- The Freedom of Information Act 2000;
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016);
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004;
- The School Standards and Framework Act 1998;
- The Protection of Freedoms Act 2012.

2.2 This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)';
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now';
- Information Commissioner's Office code of practice for the use of surveillance cameras and personal information.

2.3 This policy will be implemented in conjunction with the following other school policies:

- Student ICT & Mobile Phone Policy;
- Staff Information Systems and Social Networking Policy;
- Freedom of Information Policy;
- CCTV Policy;
- ICT Disaster Recovery Plan.

3. Applicable Data

3.1 For the purpose of this policy, personal data refers to information that relates to an identifiable, living, natural person including information such as an online identifier, such as an IP address. The Data Protection Act 2018 applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

3.2 Sensitive personal data is referred to in the Data Protection Act 2018 as 'special categories of personal data'. These specifically include the processing of genetic data, biometric data, racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual orientation and data concerning health matters.

4. Principles

4.1 In accordance with the requirements outlined in the Data Protection Act 2018, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the Data Protection Act 2018 in order to safeguard the rights and freedoms of individuals;
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4.2 The Data Protection Act 2018 also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

5. Accountability

5.1 Cox Green School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the Data Protection Act 2018.

5.2 The school will provide comprehensive, clear and transparent privacy policies.

5.3 Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

5.4 Internal records of processing activities will include the following:

- Name and details of the organisation;
- Purpose(s) of the processing;
- Description of the categories of individuals and personal data;
- Retention schedules;
- Categories of recipients of personal data;
- Description of technical and organisational security measures;
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place.

5.5 The school will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation;
- Pseudonymisation;
- Transparency;
- Continuously creating and improving security features.

5.6 Data protection impact assessments will be used, where the school brings in new initiatives or systems with high risk processing.

6. Roles and Responsibilities

6.1 The Board of Trustees

The Board of Trustees has overall responsibility for ensuring that the school complies with its obligations under all relevant data protection obligations.

6.2 The Headteacher

Day-to-day responsibilities of acting as the representative of the data controller rest with the Headteacher. Tom Smith, the IT & Facilities Operations Manager and Gill Newman, the School Business Manager also act as the Data Controllers representatives under the delegation of the Headteacher. The Headteacher will ensure that all staff are aware of their data protection obligations, and oversee the implementation of the policy.

6.3 The Data Controller

The Data Controller is Cox Green School Board of Trustees. Cox Green School pays the data protection fee required by the Information Commissioners Office.

6.4 The Data Protection Officer (DPO)

The School's DPO is: Colin Howard, Data Protection Officer, Satswana Ltd, Pembroke House, St. Christopher's Place, Farnborough, Hampshire, GU14 0NH.

The role of the DPO will be to:

- Inform and advise the school and its employees about their obligations to comply with the Data Protection Act 2018 and other data protection laws;
- Monitor the school's compliance with the Data Protection Act 2018 and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.
    - The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools.
    - The DPO will report to the highest level of management at the school, which is the headteacher.
    - The DPO will operate independently and will not be dismissed or penalised for performing their task.
    - Sufficient resources will be provided to the DPO to enable them to meet their Data Protection Act 2018 obligations.
    - The DPO is a point of contact for individual's whose data the school processes, and for the ICO.

6.5 <u>All Staff</u>

All Staff are responsible for:

- Ensuring that they collect and store any personal data in accordance with this policy;
- Informing the school of any changes to their own personal data;
- Reporting to the Headteacher if they have concerns that this policy is not being followed;
- Reporting any data breaches immediately as the DPO has to report to the ICO within 72 hours;
- Reporting if they are engaging in a new activity that may affect the privacy rights of individuals;
- Requesting guidance from the school Data Protection Team on sharing data with third parties and where necessary the appropriate Information Sharing Agreement (ISA) completed;
- Requesting authority from a member of the Senior Leadership team and the IT & Facilities Operations Manager before engaging 3rd party software or services.

7 Lawful Processing

7.1 The legal basis for processing data will be identified and documented prior to data being processed and privacy notices updated.

7.2 Under the Data Protection Act 2018, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained;
- Processing is necessary for:
    - Compliance with a legal obligation;
    - Public Task, in that the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
    - For the performance of a contract with the data subject or to take steps to enter into a contract;
    - Protecting the vital interests of a data subject or another person;

- For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

7.3 Special categories of personal data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law;
- Processing relates to personal data manifestly made public by the data subject;
- Processing is necessary for:
  - Carrying out obligations under employment, social security or social protection law, or a collective agreement;
  - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent;
  - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity;
  - Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards;
  - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional;
  - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices;
  - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

8 Consent

8.1 Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

8.2 Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

8.3 Where consent is given, a record will be kept documenting how and when consent was given.

8.4 The school ensures that consent mechanisms meet the standards of the Data Protection Act 2018. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease. Advice should be sought from the school's DPO.

8.5 Consent accepted under the DPA will be reviewed to ensure it meets the standards of the Data Protection Act 2018; however, acceptable consent obtained under the DPA will not be reobtained.

8.6 Consent can be withdrawn by the individual at any time where the information provided is voluntary.

8.7 The consent of parents will be sought prior to the processing of a child's data, except where the processing is related to preventative or counselling services offered directly to a child.

9 The Right to be Informed- Privacy Notices

9.1 The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

9.2 If services are offered directly to a child, the school will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

9.3 In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller, and where applicable, the controller's representative and the DPO;
- The purpose of, and the legal basis for, processing the data;
- The legitimate interests of the controller or third party;
- Any recipient or categories of recipients of the personal data;
- Details of transfers to third countries and the safeguards in place;
- The retention period of criteria used to determine the retention period;
- The existence of the data subject's rights, including the right to:
  - Withdraw consent at any time;
  - Lodge a complaint with a supervisory authority;
  - Object.
- The school does not use automated decision-making.

9.3 Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

9.4 Where data is not obtained directly from the data subject, information regarding the source the personal data originates from and whether it came from publicly accessible sources, will be provided.

9.5 For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

9.7 In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data;
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed;
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

10 The Right of Access

10.1 Individuals have the right to obtain confirmation that their data is being processed.

10.2 Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

10.3 The school will verify the identity of the person making the request before any information is supplied.

10.3 When a subject access request is made by a parent and the child is over 13 years old the child's permission is required for the disclosure of the information to the parent.

10.4 A copy of the information will be supplied to the individual free of charge; however, the school may charge to comply with requests for further copies of the same information. This charge will be 10p per copy.

10.5 Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

10.6 Where a request is manifestly unfounded, excessive or repetitive, we will refer to the DPO for guidance on refusal or charging.

10.7 All fees will be based on the administrative cost of providing the information – staff time cannot be charged for.

10.8 All requests will be responded to without delay and at the latest, within one month of receipt.

10.9 In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

10.10 Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

10.12 In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

See Appendix 1 for the Subject Access Request Procedure.

11. Other Data Protection Rights of the Individual

11.1 In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time where the processing relies on consent;
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances);
- Prevent use of their personal data for direct marketing;
- Challenge processing which has been justified on the basis of public interest;
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area;
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them);
- Prevent processing that is likely to cause damage or distress;

- Be notified of a data breach in certain circumstances;
- Make a complaint to the ICO;
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

16. Privacy by Design and Privacy Impact Assessments (DPIA's)

16.1 The school will act in accordance with the Data Protection Act 2018 by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into processing activities when it brings new initiatives or systems and there is high risk processing.

16.2 Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy.

16.3 DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to Cox Green School's reputation which might otherwise occur.

16.4 A DPIA will be used when using or introducing new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

16.5 High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling;
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences.

16.6 The school will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes;
- An assessment of the necessity and proportionality of the processing in relation to the purpose;
- An outline of the risks to individuals;
- The measures implemented in order to address risk.

16.7 Where a DPIA indicates high risk data processing, the school will consult its DPO and the ICO if necessary to seek its opinion as to whether the processing operation complies with the Data Protection Act 2018.

16.8 The DPIA will consider the benefits vs the impact on individual privacy and will consider if the risk can be mitigated or are there other ways to do the same thing.

17 Data Breaches

17.1 The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

17.2 The headteacher will ensure that all staff members are made aware of, and understand, what constitutes as a data breach and how to report it to the appropriate person in school as part of their continuous development training.

17.3 Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

17.4 At least all notifiable personal data breaches will be reported to the schools DPO (info@satswana.com)

17.5 All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it.

17.6 The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

17.7 In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly.

17.8 A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

17.9 In the event that a breach is sufficiently serious, the public will be notified without undue delay.

17.10 Effective and robust breach detection, investigation and internal reporting procedures are in place at the school, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

17.11 Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned;
- The name and contact details of the DPO;
- An explanation of the likely consequences of the personal data breach;
- A description of the proposed measures to be taken to deal with the personal data breach;
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects.

17.12 Failure to report a breach when required to do so will result in a fine, as well as a fine for the breach itself.

See Appendix 2 for the Personal data breach procedure

18. Data Security

18.1 Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

18.2 Confidential paper records will not be left unattended or in clear view anywhere with general access.

18.3 Digital data is protected by file permissions when stored on servers using school issued user accounts, or stored using encryption on laptops or portable storage devices.

18.4 Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

18.5 Removable storage and portable devices used to access personal data will not be used to hold personal information unless they are password-protected and fully encrypted.

18.6 All electronic devices are password-protected and portable devices encrypted to protect the information on the device in case of theft.

18.7 Staff and Trustees will not use their personal storage for school purposes.

18.8 All members of staff are provided with their own secure login and password and are prompted to change this every sixth months. All staff are required to have multi-factor authentication (MFA).

18.9 Staff who access emails on personal ~~mobile~~ portable devices must ensure their device security passcodes are alphanumeric, using upper case, special characters or numbers increases password strength. Mobile devices must have passcodes set.

18.10 Emails containing sensitive or confidential information are either sent encrypted to the recipient or password-encrypted as attachments if the recipient is outside the organisation.

18.11 Circular emails to parents are either sent via the school parental engagement app, whereby each parent receives a unique email, or are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

18.12 Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

18.13 Before sharing data, all staff members will ensure:

- They are allowed to share it;
- That adequate security is in place to protect it;
- Who will receive the data has been outlined in a privacy notice;
- The identity of the recipient has been verified.

18.14 Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.

18.15 The physical security of the school's buildings and storage systems, and access to them, is reviewed on a regular basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

18.16 Cox Green School takes its duties under the Data Protection Act 2018 seriously and any unauthorised disclosure may result in disciplinary action.

18.17 The school Business Manager is responsible for ensuring recovery measures are in place to ensure the security of protected data.

18.18 The school's servers are kept in a physically secured room, additional security measures have been put in place to prevent access, with limited key-holders.

18.19 The schools electronic data and systems are backed up regularly to a separate building within the school site. Backups are transferred to offline media in an encrypted format to be stored off site if necessary.

18.20 Cyber-attacks such as phishing attacks, trojans and ransomware are mitigated using security software and systems including anti-virus, anti-malware, firewalls, spam filters and content filters are in place to protect unauthorised access to the schools corporate network. These services are kept up to date and monitored for abnormalities.

18.21 The ICT Disaster Recovery Policy refers to steps the school takes to ensure data and systems are kept accessible and recoverable.

19. Publication of Information

19.1 Cox Green School publishes a publication scheme on its website as part of the its Freedom of Information Policy outlining classes of information that will be made routinely available, including:

- Policies and procedures;
- Annual reports;
- Financial information.

19.2 Classes of information specified in the publication scheme are made available quickly and easily on request.

19.3 Cox Green School will not publish any personal information, including photos, on its website without the permission of the affected individual.

19.4 When uploading information to the school website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

20. CCTV, Photography and Video

20.1 We use CCTV in various locations around the school site to ensure it remains safe.

20.2 We do not need to ask individuals permission to use CCTV, but cameras are clearly visible and there are signs at entrances to the site stating that CCTV is in use.

20.3 The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

20.4 The school notifies all pupils, staff and visitors of the purpose for collecting CCTV images via-CCTV policies and privacy notices.

20.5 Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

20.6 All CCTV footage will be kept for at least 32 days for security purposes; the IT & Facilities Operations Manager is responsible for keeping the records secure and allowing access.

20.7 The school will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

20.6 If the school wishes to use images/video footage of pupils in a publication, such as the school website, prospectus, or recordings of school plays, written permission will be sought from the parent of the pupil.

20.8 Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the Data Protection Act 2018.

21 Biometric Recognition Systems

21.1 Where we use pupils' biometric data as part of an automated biometric recognition system (cashless catering) we will comply with the requirements of the Protection of Freedoms Act 2012. NB: Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18

21.2 Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we process any biometric data from their child.

21.3 Parents/carers and students can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

21.4 As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

21.5 Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

22 Data Retention

22.1 Data will be retained according to the Information Management Toolkit for Schools (IRMS) and retention periods can also be found on the school's privacy notices.

22.2 Unrequired data will be deleted as soon as practicable.

22.3 Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

22.4 Paper documents will be shredded or pulped, and electronic memories scrubbed clean, deleted or destroyed, once the data should no longer be retained.

23 DBS Data

23.1 All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

23.2 Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

24. Communication of Policy

24.1 This policy will be published on the school website and the staff intranet.

25. Evidence of Implementation

25.1 The Finance & Resources Committee of the Board of Trustees will review any recommendations for action made by the DPO.

26 Review of Policy

26.1 This policy shall be reviewed every two years by the Board of Trustees through the Finance & Resources Committee.

Appendix 1 – Subject Access Request Procedure (SAR)

The Data Protection Act 2018 as set out in the Data Protection Bill 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 13 and over have their own information rights provided they are Gillick competent and in line with Fraser guidelines (they are considered mature enough to understand the data). Any subject access request made from a parent of a child aged 13 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.

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.

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 (e.g., Student Record, Personnel Record). Where the request is made by a parent or a person with parental responsibility of a student over 13 years of old the consent of the student must also be provided. In this case the request deadline will be one month from the date of receipt of the consent of the student.

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.

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 good practice to seek the consent of the third party before disclosing information. If the third party does not consent it may be necessary to seek additional advice from the DPO.

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. 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.

Data refers to paper records and all records held on computer or other mediums. A report of data held on the school information database, known as a personal data output report, should be requested via the school's IT & Facilities Operations Manager or the School Business Manager.

If the applicant wishes to make a complaint about how their SAR has been dealt with they should write to the Data Protection Officer for the school or the Chair of Trustees.

Appendix 2: Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately report the breach directly to:
    - The Headteacher, Danny Edwards;
    - The School IT & Facilities Operations Manager, Tom Smith;
    - The School Business Manager, Gill Newman;
- The DPO will be informed if the threshold is met.
- The report will be investigated and it will be determined whether a breach has occurred. To decide, consideration will be given as to whether personal data has been accidentally or unlawfully:
    - Lost;
    - Stolen;
    - Destroyed;
    - Altered;
    - Disclosed or made available where it should not have been;
    - Made available to unauthorised people.
- The Chair of Trustees will be informed of any notifiable or major data breaches.
- The DPO and Data Controllers will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure).
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data;
    - Discrimination;
    - Identify theft or fraud;
    - Financial loss;
    - Unauthorised reversal of pseudonymisation (for example, key-coding);
    - Damage to reputation;
    - Loss of confidentiality;
    - Any other significant economic or social disadvantage to the individual(s) concerned;
    - If it's likely that there will be a significant risk to people's rights and freedoms, the DPO must notify the ICO.

- The school will document the decision where it has not been referred to the ICO. The DPO will document the process for those referred to the ICO. Decisions will be recorded on the schools GDPRiS system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned;
        - The categories and approximate number of personal data records concerned.
    - The name and contact details of the DPO;
    - A description of the likely consequences of the personal data breach;
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.
- The DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO;
    - A description of the likely consequences of the personal data breach;
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- The school will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause;
    - Effects;
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).
- Records of all breaches will be stored on the schools GDPRiS system.
- The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to Minimise the Impact of Data Breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Special Categories of Personal Data Being Disclosed via Email (Including Safeguarding Records):

- Information containing special categories of personal data must be sent as a password protected document;
- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error;
- Members of staff who receive personal data sent in error must alert the sender and the Data Protection Team as soon as they become aware of the error;
- If the sender is unavailable or cannot recall the email for any reason, the school will ask the IT Support department to recall it. This relates to internally sent mail only;
- In any cases where the recall is unsuccessful, the School will contact the relevant un-authorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way;
- The School will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request;
- The school will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

Details of Pupil Premium Interventions for Named Children Being Published on the School Website

- If personal data is accidentally made available through public websites, the owner of the webpage must take immediate steps to ensure the data is removed by contacting the website owner or administrator.
- The member of staff aware of the breach must alert the Data Protection Team as soon as they become aware of it.
- The school will carry out an internet search to check that the information has not been further disseminated on the internet; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

Non-Anonymised Pupil Exam Results or Staff Pay Information Being Shared With Trustees

- All papers circulated to Trustees will be checked by the writer and the Clerk to Trustees to ensure that no personal data or special category data is included in the papers.
- If personal or special category data is shared with Trustees, the Trustee/member of staff who becomes aware of the data breach must alert the Data Protection Team as soon as they become aware of it.
- The school must contact all recipients of the information and ask them to delete the information and not share, publish, save or replicate it in any way.

- The school will ensure a written response is received from all the individuals who received the data, confirming that they have complied with this request.
- The school will ask the writer of the papers to re-issue them with the personal data or special category data removed.

A School Laptop or USB Containing Non-Encrypted Sensitive Personal Data Being Lost, Stolen or Hacked

- The member of staff must inform the School Data Protection Team or the Headteacher as soon as they become aware of the loss, theft or hacking.
- The Data Protection team or the Headteacher will alert the Data Protection Team as soon as they become aware of the breach.
- The school must alert the police of the loss if appropriate and take all possible steps available to them to retrieve the data.
- The school, where possible, will enable remote blocking.
- The school, to establish whereabouts of the bit locker.
- The school must make the owner of the personal data, if any is lost, stolen or hacked, aware of the loss of the data.
- The school will carry out an internet search to check that the information has not been disseminated on the internet; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted