Crompton House
C of E Multi Academy Trust

Data Protection Policy

Contents

1. Aims

Crompton House Church of England Multi Academy Trust aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Act 2018 (DPA2018). This policy applies to all personal data, regardless of whether it is in paper or electronic format.

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with relevant legislation.

This policy should be read in conjunction with the Records Management Policy and The Child Protection Policy. For the sake of clarity, any mention of the 'The Trust' or 'The Trust' includes staff working in any of the Crompton House Multi Academy Trust academies.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

3. Scope of the Policy

This policy applies to the Trust Board of Directors, school governors, staff, pupils and any individuals about whom the school processes personal information, as well as other partners and companies with which the school undertakes business.

The Trust as a body corporate is the Data Controller under the 2018 Act (the Act). However, the Data Protection Officer will deal with day to day matters. Any member of staff, pupil or any other individual who considers that the policy has not been followed in respect of personal data about himself or herself should raise the matter with the Data Protection Officer. The Data Protection Officer for the Trust is Debbie Burgess.

Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred in the first instance to the DPO. dpo@cromptonhouse.org

This policy has been adopted by the Trust Board and is a detailed statement of policy regarding one main area of information management. It does not form part of the formal contract of employment for staff or a formal offer of a place of study for pupils. However, this policy will be included in the staff handbook and it is a condition of employment that employees will abide by the rules and policies made by the Trust from time to time. Any failure to follow the policy can, therefore, result in disciplinary proceedings.

4. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.

Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

5. The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others and therefore is a data controller.

The Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required for all our and associate schools.

6. Data protection principles

The Trust needs to keep certain information about its employees, pupils, their parents and other individuals who come into contact with the academy in order provide education and associated functions in order to allow it to monitor performance, achievements and health and safety and seek to achieve its aims (as set out in the commitment statement). In so doing, the Trust and its academies will comply with the terms of the Data Protection Act 2018 and any associated legislation, to ensure personal data is treated in a manner that is fair and lawful.

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how The Trust aims to comply with these principles.

In addition to this, The Trust is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the Rights of Individuals under the law (as explained in more detail in below)

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given explicit consent
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for the establishment, exercise or defence of legal claims
- The data needs to be processed for reasons of substantial public interest as defined in legislation
- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given consent
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent

- The data has already been made manifestly public by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- The data needs to be processed for reasons of substantial public interest as defined in legislation

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with The Trusts Records Management Policy.

7.3 Types of Personal Data Processed by The Trust

Personal data covers both facts and opinions about an individual. The Trust may process a wide range of personal data about individuals including current, past and prospective pupils and their parents as part of its operation, including, by way of example:

- Legal and preferred name, date of birth, gender, addresses, telephone numbers, email addresses and other contact details, ethnicity, nationality, first language, country of birth, religion, pupil premium and free school meals information and travel arrangements.
- Past, present and prospective pupils' academic, disciplinary, admissions and attendance
- Records (including information about any special needs), and examination scripts and marks
- Where appropriate, information about individuals' health, and contact details for their next of kin and doctor
- References given or received by the School about pupils, and information provided by previous educational establishments and/or other professionals or organisations working with pupils; and
- Images of pupils (and occasionally other individuals) engaging in School activities, and
- Images captured by the School's CCTV system (in accordance with The Trusts Policy on taking, storing and using images of children)
- Test and Assessment data
- Pastoral Support records including welfare information, Incident and accident forms, communications to and from home, Admissions documents, Exclusion documentation, detention and behaviour records, Attendance records, Education Health Care Plan (EHCP) and Safeguarding records

Generally, The Trust receives personal data from the individual directly (or, in the case of pupils, from parents). However in some cases personal data may be supplied by third parties (for example another School, or other professionals or authorities working with that individual), or collected from publicly available resources.

Your data is stored on the individual school's management information system which is Progresso who uphold the same data protection standards as the school. Any paper records are then scanned and uploaded to the pupil record within our system and then confidentially destroyed.

7.4 Data Gathering

All personal data relating to staff, pupils or other people with who we have contact, whether held on computer or in paper files, are covered by the Act.

Only relevant personal data may be collected and the person from whom it is collected must be informed of the intended use of the data (only if that person is the data subject) and of any possible disclosures of that information which may be made.

7.5 Data Checking

The Trust and academies will issue regular reminders at the beginning of the academic year to staff and parents to ensure that personal data held is up-to-date and accurate.

8. Roles and Responsibilities

All staff are responsible for:

- checking that any information which they provide to the Trust in connection with their employment is accurate and up-to-date; and
- informing the Trust of any changes to information they have provided, e.g. change of address, either at the time of appointment or subsequently. The Trust cannot be held responsible for any errors unless the staff member has informed the Trust of such changes

Responsibility of Parents

Pupils and their parents should ensure that all personal information provided to the academy and the Trust is accurate and up-to-date. They should ensure that changes of address, etc. are notified to the academy. The Trust cannot be held responsible for any errors unless the parent has informed the academy of such changes. Subject to the above, any errors discovered will be rectified and, if the incorrect information has been disclosed to a third party, they will be informed of the corrected data.

9. Sharing personal data

The Trust and its academies may receive requests from third parties to disclose personal data it holds about pupils, their parents or guardians. Personal data will only be disclosed to organisations or individuals where the Trust has consent to do this, or where there is a legal requirement to make the disclosure without consent.

When requests to disclose personal data are received by telephone, it is the legal responsibility of the academy to ensure that the academy is entitled to disclose the data and that the organisation is who it says it is. Therefore, such requests should be referred to the Data Protection Officer and School Business Manager or equivalent who will normally ask for the request in writing. A record should be kept of any personal data disclosed so that the recipient can be informed if the data is later to be found to be inaccurate. This will also enable an audit trail to be created across the Trust.

Personal data will not be used in newsletters, websites or other media without the consent of the data subject.

Routine consent issues are incorporated into the academy and Trust's pupil and staff data gathering sheets to avoid the need for frequent similar requests for consent being made by the academy. This will include information considered sensitive (special category) under the Act relating to particular health needs, such as allergies or medical conditions. The academy will only use this information in the protection of the health and safety of the individual, but requires consent to process this data in the event of a medical emergency.

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies.

When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9.1 Keeping in touch

We will use the contact details of parents, alumni and other members of the School community to keep them updated about the activities of the School, including sending updates and newsletters, by email and by post. Unless the relevant individual objects, the School may also:

- Share personal data about parents and/or alumni and other members of the school community such as Parents, Teachers and Friends Association.

- Contact parents and/or alumni by post and email in order to promote and raise funds for the school and, where appropriate, other worthy causes.
- Should you wish to limit or object to any such use, or you would like further information about them please contact the DPO in writing.

10. Subject access requests and other rights of individuals

10.1 Subject access requests

All people for whom the Trust holds personal information are entitled to access to their personal data as follows:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

A request to access this data is known as a subject access request or SAR. Any request either in writing, by email or verbally is a SAR. If staff receive a subject access request they must immediately forward it to the DPO.

10.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child aged 12 and above, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from parents or carers of pupils under the age of 12 may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

10.3 Responding to subject access requests

When responding to requests, we:

- Will ask the individual to provide a form of identification such as a current passport, driving license or recent utility bill with current address
- Will request completion of the SAR request form
- Will respond without delay and within 1 month of receipt of the SAR request form
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

Where the information sought contains the personal data of a third party then we will consider whether it is possible to redact information so that this does not identify those third parties. If this is not possible, consider whether the consent of those third parties can be obtained. If consent has been refused, or it is not considered appropriate to seek that consent, then we will consider whether it would be reasonable in the circumstances to disclose the information relating to those third parties. If it is not then the information may be withheld.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

10.4 Other data protection rights of the individual

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
- 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)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

11. Parental requests to see the educational record

In academies there is no legal right for parents, or those with parental responsibility, to access their child's educational record. In deciding whether to grant such a request the academy may consult with the child if aged 12 or above.

Request for Educational records.

The school can charge what it costs to supply a copy of the information in an Educational Record.

12. Photographs and videos

As part of The Trust and its academies activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our child protection and safeguarding policy for more information on our use of photographs and videos.

13. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)

- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. Data security and storage of records

The Trust will take appropriate technical and organisational steps to ensure the security of personal data about individuals, and to ensure that members of staff will only have access to personal data relating to pupils, their parents or guardians where it is necessary for them to do so. All staff will be made aware of this policy and their duties under the Act.

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must follow the procedures within their individual academy.
- Only passwords which prescribe to protocols set out in the IT Acceptable Use and GDPR policy may be used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices and permission is sought from IT/Business Manager prior to use
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

15. Disposal of records

Personal data will be retained for no longer than is necessary for the purpose for which it was collected. Standard retention times are necessary to meet various contractual requirements.

Standard retention times are specified in the Trust Document Retention Policy.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files or use a suitable professional confidential waste company that provides certificates of destruction. If we use a thirty party, we will require the third party to provide sufficient guarantees that it complies with data protection

15.1 The Independent Inquiry into Child Sexual Abuse

The Independent Inquiry into Child Sexual Abuse (formerly The Goddard Inquiry) was launched at the beginning of July 2015. The Inquiry is investigating whether public bodies and other non-state institutions have taken seriously their duty of care to protect children from sexual abuse in England and Wales. Judge Goddard made it very clear in her opening statement the importance of retaining records. She wrote to institutions including local authorities and religious organisations on the subject of retaining records but confirmed that the content of those letters should be taken to apply to all institutions which have had responsibility for the care of children.

In view of Judge Goddard's clear direction to institutions not to destroy records, the School will not destroy pupil records after the customary seven year period, as determined by the DPO in accordance with the Data Protection Principles published by the Information Commissioner's Office, but will retain them and all staff records until the Inquiry has concluded. The Inquiry supercedes any data protection legislation.

16. Personal data breaches

The trust and its associated academies will make all reasonable steps to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours.

17. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

18. Monitoring arrangements

This policy will be reviewed every 2 years and shared with the full governing board.

19. Complaints

If an individual believes that the School has not complied with this Policy or acted otherwise than in accordance with the Act, they should utilise the School's complaints procedure and should also notify the DPO.

Complaints about the operation of the procedures should be made to the DPO who will decide if it is appropriate for the complaint to be dealt with under the complaints procedure. Complaints which are not dealt with under the school's complaint procedure should be forwarded in writing to the Information Commissioner. It is likely that complaints about procedural issues, due process and timeliness will be dealt with by the trustees, complaints that involve consideration of personal data or sensitive personal data should be referred to the Information Commissioner.

20. Links with other policies

This policy is relevant to all strategies, policies, procedures, codes, guides etc dealing with information management, personnel, social care, education, information security, Freedom of Information, Environmental Information Regulations, records management and complaints.

Appendix 1: 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 notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider 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 DPO will alert the Headteacher and/or the Business Manager
- The DPO 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 risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in the schools DPA documentation.
- 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

- If all the above details are not yet known, 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 DPO 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 within the schools DPA documentation.
- The DPO and Headteacher or Chief Executive Officer (if significant breach) will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.
- Significant breaches are to be reported to the Trust Board

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.

Sensitive information being disclosed via email (including safeguarding records)

- 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 DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it

- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised 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 DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO 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