COCKBURN
MULTI-ACADEMY TRUST
TRANSFORMATION TO EXCELLENCE

Data Protection Policy

(in line with The UK General Data Protection Regulation (GDPR)

Reviewed by: The Board

Date of Policy: July 2020

To be reviewed: September 2022

Contents

1. **Introduction**
2. **Roles and responsibilities**
3. **Our promise**
4. **Collecting personal data**
5. **Subject Access Requests – Requesting Information**
6. **Other Rights**
7. **Access to data and disclosure**
8. **Location of information and data security**

Appendix 1: definitions
Appendix 2: personal data breach procedure
Appendix 3: data breach reporting form

1. Introduction

Cockburn Multi-academy Trust is committed to being transparent about how it collects and uses the personal data of its workforce and students, and to meeting its data protection obligations. This policy sets out our commitment to data protection, and individual rights and obligations in relation to personal data. Changes to UK data protection legislation (GDPR May 2018) shall be monitored and implemented in order to remain compliant with all requirements.

This policy applies to the personal data of job applicants, employees, (workers, contractors, volunteers, apprentices) and former employees, and to students and former students of any school within the MAT, regardless of whether it is in paper or electronic format.

Cockburn MAT believes that protecting the privacy of our staff and students and regulating their safety through data management, control, and evaluation is vital to whole-school and individual progress. The school collects personal data from students, parents/carers, and staff and processes it in order to support teaching and learning, monitor and report on student and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the school will keep parents/carers fully informed of the how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all that we can to support both staff and students. The legal basis for processing data is that it is necessary to carry out these tasks in the public interest.

Cockburn MAT is also committed to ensuring that its staff, governors and trustees are aware of data protection policies, legal requirements and ensuring adequate training is provided. The requirements of this policy are mandatory for all staff employed by the school and to external organisations or individuals working on our behalf.

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

2. Roles and Responsibilities:

2.1 MAT Board/Governing Bodies

The MAT Board have responsibility to ensure that Cockburn MAT complies with all relevant data protection obligations. Individual governing bodies has overall responsibility for ensuring that each individual school complies with all relevant data protection obligations.

2.2 Data protection officer
The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with UK data protection law, and developing related policies and guidelines where applicable.

They will provide advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO. The DPO for Cockburn MAT is Sharon Burns and is contactable via email. The DPO will be supported by nominated individuals in each school.

2.3 Headteachers/Heads of School

The Executive Head acts as the representative of the data controller on a day-to-day basis for the multi-academy trust data.

The Headteacher/Head of School acts as the representative of the data controller on a day-to-day basis in his/her school.

2.4 All staff

Staff are responsible for helping to keep their personal data up to date. Individuals must let their school's know if data previously provided changes, for example if an individual moves house or changes their bank details. All schools within Cockburn MAT will update personal data promptly with both the school direct, Leeds City Council payroll and the appropriate Pensions company, if they are advised that their information has changed or is inaccurate.

Staff are responsible for:

- collecting, storing and processing any personal data in accordance with this policy
- informing the school of any changes to their personal data, such as a change of address
- contacting the DPO in the following circumstances:
    - with any questions about the operation of this policy, UK data protection law, retaining personal data or keeping personal data secure
    - if they have any concerns that this policy is not being followed
    - if they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - if they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
    - if there has been a data breach
    - whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - if they need help with any contracts or sharing personal data with third parties

Some staff may have access to the personal data of other individuals [staff and students] in the course of their employment or placement. Where this is the case, we rely and expect staff to help meet our data protection obligations.

Staff who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

Failing to observe these requirements may amount to a disciplinary offence. Significant or deliberate breaches of this policy, such as accessing employee or student data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Staff personal data gathered during the employment or placement, is held in an individual's personnel file (in hard copy and electronic format), and on HR systems and documents. The periods for which this information is held will be contained in privacy notices. Cockburn MAT will keep a record of its processing activities in respect of personal data in accordance with the requirements of the General Data Protection Regulation (UK GDPR).

3. Our promise

All data within the MAT and individual school's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

In line with the Data Protection Act 1998, and following principles of good practice when processing data, all schools within the MAT will:

- ensure that data is fairly and lawfully processed
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive
- ensure that data processed is accurate
- not keep data longer than is necessary
- process the data in accordance with the data subject's rights
- ensure that data is secure
- ensure that data is not transferred to other countries without adequate protection.

4. Collecting personal data

4.1 Fair Processing / Privacy Notice:

We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and students prior to the processing of individual's data.

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under UK 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 student) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018.

4.2 Sharing Personal Data

We will not normally share data, there may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities, for example our local authority, Ofsted, or the department of health. These authorities are up to date with UK data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of the MAT shall be clearly defined within notifications and details of the basis for sharing given. Data will only be shared with external parties in circumstances where there is an issue with a student 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 students – for example, IT companies. When doing this, we will:
    - only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK 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 students or staff. Where we transfer personal data to a country or territory outside the UK, we will do so in accordance with UK data protection law.

Under no circumstances will the school disclose information or data:

- that would cause serious harm to the child or anyone else's physical or mental health or condition
- indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child
- that would allow another person to be identified or identifies another person as the source, unless the person is an employee of the school or local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed
- is contained in adoption or parental order records
- is given to a court in proceeding concerning the child

5. Subject Access Request – Requesting Information

All individuals including students whose data is held by Cockburn MAT, have a legal right to request access to such data or information about what is held.

This includes:

- 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 must be submitted in writing, either by letter, email or fax to the DPO. They should include:

- name of individual
- correspondence address
- contact number and email address
- details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents/carers. For a parent/carer to make a subject access request with respect to their child, 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, most subject access requests from parents/carers of students at our school may be granted without the express permission of the student. Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents/carers of students at our school may not be granted without the express permission of the student. These are not rules and a student ability to understand their rights will always be judged on a case-by-case basis and we will bear in mind guidance issued from time to time from the Information Commissioner's Office.

Educational record

A student can request, in writing, to see their educational record. This record may include:

- a statement of special educational needs
- their personal education plan (PEP) – the document provided by social care to the school if a child is looked-after
- a record of information kept by the school, for example relating to behaviour or family background, which:
  - is processed by or on behalf of the governing body or a teacher at any maintained or special school
  - relates to a past or present student
  - originates from any employee at the LA that maintains the school, or is supplied by or on behalf of them
  - originates from any teacher or other employee at the student's school or former school or is supplied by or on behalf of them
  - originates from the student to whom the record relates or the student's parent/carer, or is supplied by or on behalf of them

Staff

We are legally obliged to protect certain information on our staff. School staff have a right to see records of their personal information. Staff who wish to access this information can make a subject access request under the Data Protection Act 1998. Disclosure of these records will be made once third party information has been removed in accordance with the Data Protection Act 1998.

Responding to subject access requests
When responding to requests, we:

- may ask the individual to provide 2 forms of identification
- may contact the individual via phone to confirm the request was made
- will respond without delay and within 1 month of receipt of the request
- 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.

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

6. Other rights

Individuals including students have a number of other rights in relation to their personal data. They can:

- 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 UK
- 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.

7. Access to data and disclosure

Third parties

Personal data about students will not be disclosed to third parties without the consent of the child's parent/carer, unless it is obliged by law, required to support the provision of education or in the best interest of the child. Data may be disclosed to the following third parties without consent:

- **Other schools**
  If a student transfers from one of our schools in the trust to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.

- **Examination authorities**
  This may be for registration purposes, to allow the students at our school to sit examinations set by external exam bodies.

  The information supplied to the school will be used by the Skills Funding Agency, an executive agency of the Department for Education (DfE), to issue students with a Unique Learner Number (ULN), and to create a Personal Learning Record. For more information about how information is processed and shared students can refer to the Extended Privacy Notice available on Gov.UK.

- **Health authorities**
  As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

- **Police and courts**
  If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

- **Social workers and support agencies**
  In order to protect or maintain the welfare of our students, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

- **Educational division**
  Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce the Education Act.

Biometric recognition systems

Where we use students' biometric data as part of an automated biometric recognition system (for example, students use finger prints to receive school dinners instead of paying with cash, we will comply with the requirements of the Protection of Freedoms Act 2012).

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

Parents/carers and students have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those students.

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.

As required by law, if a student 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 student's parent(s)/carer(s).

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 any relevant data already captured will be deleted.

CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to Sharon Burns Chief Operating Officer. For more information on CCTV please refer to the separate CCTV policy.

Photographs and videos

As part of our school activities, we may take photographs and record images of individuals. Images of staff and students may be captured at appropriate times and as part of educational activities for use in school only. It is the school's policy that external parties (including parents) may not capture images of staff or students during such activities without prior consent.

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

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/photography policy/other relevant policy] for more information on our use of photographs and videos.

School staff
School staff will have restricted access to students' personal data and will be given access only on a 'need to know' basis in the course of their duties within the school. All staff are well informed of the Data Protection Act and how their conduct must correspond with this. Staff will use data only for the purpose of which it was collected, and any staff that are found to be acting intentionally in breach of this will be disciplined in line with the seriousness of their misconduct.

8. Location of information and data security

Cockburn Multi-academy Trust takes the security of personal data seriously. The organisation has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

In particular:

Hard copy data, records, and personal information should be stored out of sight and in a locked cupboard no matter what format it is in. The only exception to this is medical information that may require immediate access during the school day. This will be stored with the school nurse/main first aider.

Electronic records – access will only be given to folders where there is a legitimate business reason to have access.

Sensitive or personal information and data should ideally not be removed from the school site, however the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with students. The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.
- unwanted paper copies of data, sensitive information or student files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or student by name.
- care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
- if information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.
- if it is necessary to transport data away from the school, it should be downloaded onto an encrypted USB stick. The data should not be transferred from this

encrypted USB stick onto any home or public computers. Work should be edited from the encrypted USB stick, and saved onto the encrypted USB stick only.
- all documents holding personal data sent electronically should at least be password protected.
- 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
- clear desk policy - 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
- passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff 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
- staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our [online safety policy/ICT policy/acceptable use agreement/policy on acceptable 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)

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them. Risk and impact assessments shall be conducted in accordance with guidance given by the ICO performance.

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of the misconduct.

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 UK 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

Retention of data

Individual schools within the MAT will not keep personal data on students for any longer than is necessary. Information such as statistical data, and information that is collected to be kept as part of school records, will be kept by the school even after the child leaves.

It is very important that all examination results certificates and records indicating the progress of a student are safely kept by their parents/carers as the school cannot guarantee that this information will be kept indefinitely by the school.

The school cannot guarantee that any information will be kept by the school indefinitely, although records are usually kept for a period of 7 years after the child has left the school. All student and staff records will be retained in line with the Information and Records Management Society Retention Guidelines for Schools.

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with UK data protection law.

Personal data breaches

We will make all reasonable endeavours 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 3.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- a non-anonymised dataset being published on the school website which shows the exam results of students eligible for the student premium
- safeguarding information being made available to an unauthorised person
- the theft of a school laptop/device containing non-encrypted personal data about students

Staff must inform the data protection officer of any breach. If the breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures we have taken as a result.

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.

Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full governing body and MAT Board

Appendix 1: 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.

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 notify the DPO using the data breach form at Appendix 3
- 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 Executive Headteacher, Headteacher/Head of School and the Chair of Governors
- 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, on the school's computer 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
- 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 [set out where you will keep these records – for example, on the school's computer system, or on a designated software solution]
- The DPO and Executive 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.

For example:

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*

Other types of breach that you might want to consider could include:

- *Details of student premium interventions for named children being published on the school website*
- *Non-anonymised student exam results or staff pay information being shared with governors*
- *A school laptop containing non-encrypted sensitive personal data being stolen or hacked*
- *The school's cashless payment provider being hacked and parents' financial details stolen*

Appendix 3: Data Breach Reporting Form

Date:		**Person reporting breach**		
Outline of Breach				
Which data subjects were involved				
Data Type involved				
Phone/email sent to DPO	**Yes/No**	**Is this high risk?**	**Please explain**	**Report to ICO** **Yes/No**
Date reported to				
Actions Taken				
Preventative actions taken				
Notes				
Signed off by DPO			**Date**	