Centre Academy East Anglia

Data Protection Policy

Equality Statement

Centre Academy East Anglia is committed to a policy of equality and aims to ensure that no employee, job applicant, pupil or other member of the school community is treated less favourably on grounds of sex, race, colour, ethnic or national origin, marital status, age, sexual orientation, disability or religious belief. We provide a safe, supportive and welcoming environment

Review Date:	April 2026
Last Review Date:	April 2025
Held on website:	Yes

Signed by Chair of Proprietor Body

Signed: **Date: 23/04/25**

Chair of Proprietor Body **Mr R Murphy**

Centre Academy East Anglia is committed to safeguarding and promoting the welfare of children and young people and expects all staff to share this commitment.

Contents

1. Aims

Our school 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 UK data protection law.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR

- CCTV – If in use it also reflects the ICO's code of practice for the use of surveillance cameras and personal information.
- In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living 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.

4. The Data Controller

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

The school is registered with the ICO and has paid its data protection fee to the ICO (ICO Registration Number: Z7451143), as legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governance

The Governance Team has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data Manager

The Data Manager is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the Governance and, where relevant, report to the board their advice and recommendations on school data protection issues.

The Data Manager is also the first point of contact for individuals whose data the school processes, and for the ICO.

Our Data Manger is the proprietor and is contactable via the school office. Questions regarding personal data or its use should be directed to the Data Manager through the School Office.

The headteacher acts as the representative of the data controller on a day-to-day basis.

5.3 All staff

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 Data Manager in the following circumstances:
    - With any questions about the operation of this policy, 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 European Economic Area
    - 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

6. Data protection principles

The UK 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 school aims to comply with these principles.

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 or another person i.e. 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 or exercise its official authority**
- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) 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 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

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

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.

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.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

In addition, 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 school's record retention schedule.

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations 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 contract with the supplier or contractor 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

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

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 internationally, we will do so in accordance with data protection law.

9. Data Protection Requests (Subject access requests and other rights of individuals)

9.1 Data Protection Requests (Subject access requests)

Individuals have a right to make a 'Data Protection Request (subject access request)' to gain access to personal information that the school holds about them. 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
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- 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

- The safeguards provided if the data is being transferred internationally

Data Protection Request (subject access requests) can be submitted in any form (Please see ***appendix 2***, but we may be able to respond to requests more quickly if they are made in writing and include:

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

If staff receive a Data Protection Request (subject access requests) in any form they must immediately forward it to the Data Manager.

9.2 Children and Data Protection Request (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 Data Protection Request (subject access request) with respect to their child, the child must either be unable to understand their rights and the implications of a Data Protection Request (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 or carers of pupils at our school 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.

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 or carers of pupils at our school may not 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.

9.3 Responding to Data Protection Requests (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 (or receipt of the additional information needed to confirm identity, where relevant)
- 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 may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their Data Protection Request (subject access request) right through the courts.

9.4 Other data protection rights of the individual

In addition to the right to make a Data Protection Request (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 (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- 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 Data Manager. If staff receive such a request, they must immediately forward it to the Data Manager.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. CCTV

When in use, CCTV is 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 Data Manager.

12. Photographs and videos

As part of our school 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.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils 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 pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly

on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Where the school takes photographs and videos, 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.

13. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. Centre Academy East Anglia recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Centre Academy East Anglia will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1.

14. 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 Data Manager, 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 data protection 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 Data Manager 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
- Appropriate safeguards being put in place if we transfer any personal data outside of the European Economic Area (EEA), where different data protection laws will apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and Data Manager and all information we are required to share about how we use and process their personal data (via our privacy notice)
    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the EEA and the safeguards for those, retention periods and how we are keeping the data secure

15. Data security and storage of records

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 sign it in and out from the school office
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils 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 E-Safety (Online Safeguarding Policy/ICT Acceptable Use Agreement/CAEA Handbook for Faculty Staff).
- 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)

16. Disposal of records

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 data protection law.

17. Personal data breaches

The school 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 1.***

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. 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 pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

18. Data Protection Impact Assessment (DPIA)

Completion of a Data Protection Impact Assessment (DPIA) is a requirement of Article 35 of the General Data Protection Regulation. A Data Protection Impact Assessment (**DPIA**) is a process to help you identify and minimise the data protection risks of a project. A **DPIA must be completed** for processing or changes to existing processing that are likely to result in a high risk to individuals.

With so much information being collected, used and shared in the school, it is important that steps are taken to protect the privacy of each individual and ensure that personal information is handled legally, securely, efficiently and effectively.

Completion of a DPIA will assist us to identify and minimise our privacy risks to comply with our data protection obligations and meet individuals' expectations of privacy. (Appendix 3).

19. Training

All staff 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.

20. Monitoring arrangements

The Data Manager is responsible for monitoring and reviewing this policy.

This policy will be reviewed when it is required (legislation is changed) and shared with the Governance Team.

21. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- E-Safety (Online Safeguarding Policy)
- Data Protection for Staff
- Child Protection and Safeguarding Policy
- Data Protection Privacy Notice

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 Data Manager
- The Data Manager will investigate the report, and determine whether a breach has occurred. To decide, the Data Manager 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 Data Manager will alert the CEO/Principal and the Governance Team.
- Staff will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, the Data Manager will alert the Governance.
- The Data Manager will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary and the Data Manager should take external advice when required (e.g. from IT providers). (actions relevant to specific data types are set out at the end of this procedure)
- The Data Manager will assess the potential consequences, based on how serious they are, and how likely they are to happen before and after the implementation of steps to mitigate the consequences.
- The Data Manager will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
- The Data Manager 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 Data Protection file held in the PA/Secretary to School's Office.
- Where the ICO must be notified, the Data Manager will do this via the 'report a breach' page of the ICO website, or through their breach report line (0303 123 1113), within 72 hours. As required, the Data Manager 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 Data Manager
    - 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 Data Manager 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 Data Manager expects to have further information. The Data Manager will submit the remaining information as soon as possible
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach
    - 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 consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The Data Manager will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts relating to the breach
    - 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 in Data Protection file held in the Office Manager's Office.
- The Data Manager will meet with the CEO/Principal 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 set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, 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 Data Manager as soon as they become aware of the error.

  If the sender is unavailable or cannot recall the email for any reason, the Data Manager will ask the external IT support provider to attempt to recall it from external receipients and remove it from the school;s email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the Data Manager will consider whether it's appropriate to 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 Data Manager will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The Data Manager 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
- If safeguarding information is compromised, the Data Manager will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners

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

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil 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
- Hardcopy reports sent to the wrong pupils or families

Internal Recording

Records of data breaches will be kept and stored securely in the Head of School's office.

Data Breach Incident Report Form

Description of the Data Breach:	
Time and Date breach was identified and by whom.	
Who is reporting the breach:	
Contact details: **Telephone/Email**	
Classification of data breached i. Public Data ii. Internal Data iii. Confidential Data iv. Highly confidential Data	
Volume of data involved	
Confirmed or suspected breach?	
Is the breach contained or ongoing?	
If ongoing what actions are being taken to recover the data	
Who has been informed of the breach	
Any other relevant information	
Received by:	
Date/Time:	

Completed form to be handed to the Data Manager

Evaluation of Incident Severity

The severity of the incident will be assessed by the Data Manager

Assessment would be made based upon the following criteria:

High Criticality: Major Incident	**Contact:**
• Highly Confidential/Confidential Data • Personal data breach involves > 1000 individuals • External third party data involved • Significant or irreversible consequences • Likely media coverage • Immediate response required regardless of whether it is contained or not • Requires significant response beyond normal operating procedures	Lead Responsible Officer • To be determined by Data Manager Other relevant contacts • Governance • Internal SMT as required • Contact external parties as required ie police/ICO/individuals impacted
Moderate Criticality: Serious Incident	**Contact:**
• Confidential Data • Not contained within School • Breach involves personal data of more than 100 individuals • Significant inconvenience will be experienced by individuals impacted • Incident may not yet be contained • Incident does not require immediate response • Incident response may require notification to SMT	Lead Responsible officer • Data Manager, Department affected by the incident Other relevant contacts: • Chief Information Officer • Governance
Low Criticality: Minor Incident	**Contact:**
• Internal or Confidential Data • Small number of individuals involved • Risk to School low • Inconvenience may be suffered by individuals impacted • Loss of data is contained/encrypted • Incident can be responded to during working hours Example: Email sent to wrong recipient Loss of encrypted mobile device	• Data Manager (May delegate responsibility to another appropriate SMT member) Other relevant contacts: • ICT Department • Governance Team to follow up on policy procedures for managing personal data breaches

Data Breach Checklists

A. Containment and Recovery
B. Assessment of Risks
C. Consideration of Further Notification
D. Evaluation and Response

Step	Action	Notes
A	**Containment and Recovery:**	**To contain any breach, to limit further damage as far as possible and to seek to recover any lost data.**
1	Data Manager to ascertain the severity of the breach and determine if any personal data is involved.	**See Appendix 2**
2	Data Manager to investigate breach and forward a copy of the data breach report	Data Manager to oversee full investigation and produce report. Ensure lead has appropriate resources including sufficient time and authority. If personal data has been breached Data Manager will lead the initial response.
3	Identify the cause of the breach and whether the breach has been contained? Ensure that any possibility of further data loss is removed or mitigated as far as possible	Establish what steps can or need to be taken to contain the breach from further data loss. Contact all relevant staff who may be able to assist in this process. This may involve actions such as taking systems offline or restricting access to systems to a very small number of staff until more is known about the incident.
5	Determine whether anything can be done to recover any losses and limit any damage that may be caused	E.g. physical recovery of data/equipment, or where data corrupted, through use of back-ups.
6	Where appropriate, the Data Manger will inform the police.	E.g. stolen property, fraudulent activity, offence under Computer Misuse Act.
7	Ensure all key actions and decisions are logged and recorded on the timeline.	

Step	Action	Notes
B	**Assessment of Risks**	**To identify and assess the ongoing risks that may be associated with the breach.**
8	What type and volume of data is involved?	Data Classification/volume of individual data etc
9	How sensitive is the data?	Sensitive personal data? By virtue of definition within Data Protection Act (e.g. health record) or sensitive because of what might happen if misused (banking details).
10	What has happened to the data?	E.g. if data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk.
11	If the data was lost/stolen, were there any protections in place to prevent access/misuse?	E.g. encryption of data/device.
12	If the data was damaged/corrupted /lost, were there protections in place to mitigate the impact of the loss?	E.g. back-up tapes/copies.
13	How many individuals' personal data are affected by breach?	
14	Who are the individuals whose data has been compromised?	Students, applicants, staff, customers, clients or suppliers?
15	What could the data tell a third party about the individual? Could it be misused?	Consider this regardless of what has happened to the data. Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.
16	Is there actual/potential harm that could come to any individuals?	E.g. are there risks to: • physical safety; • emotional wellbeing; • reputation; • finances; • identify (theft/fraud from release of non-public identifiers); • or a combination of these and other private aspects of their life?
17	Are there wider consequences to consider?	E.g. a risk to public health or loss of public confidence in an important service we provide?
18	Are there others who might advise on risks/courses of action?	E.g. If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

Step	Action	Notes
C	**Consideration of Further Notification**	**Notification is to enable individuals who may have been affected to take steps to protect themselves or allow the regulatory bodies to perform their functions.**
19	Are there any legal, contractual or regulatory requirements to notify?	E.g.: terms of funding; contractual obligations
20	Can notification help the School meet its security obligations under the seventh data protection principle?	E.g. prevent any unauthorised access, use or damage to the information or loss of it.
21	Can notification help the individual?	Could individuals act on the information provided to mitigate risks (e.g. by changing a password or monitoring their account)?
22	If a large number of people are affected, or there are very serious consequences, inform the Information Commissioner's Office	Data Manger to inform Governance and contact ICO
23	Consider the dangers of 'over notifying'.	Not every incident will warrant notification "and notifying a whole 2 million strong customer base of an issue affecting only 2,000 customers may well cause disproportionate enquiries and work".
24	Consider whom to notify, what you will tell them and how you will communicate the message.	• There are a number of different ways to notify those affected so consider using the most appropriate one. Always bear in mind the security of the medium as well as the urgency of the situation. • Include a description of how and when the breach occurred and what data was involved. Include details of what has already been done to respond to the risks posed by the breach. • When notifying individuals give specific and clear advice on the steps they can take to protect themselves and also what the institution is willing to do to help them. • Provide a way in which they can contact us for further information or to ask questions about what has occurred (e.g. a contact name, helpline number or a web page).
25	Consult the ICO guidance on when and how to notify it about breaches.	Where there is little risk that individuals would suffer significant detriment, there is no need to report. There should be a presumption to report to the ICO where a large volume of personal data is concerned and there is a real risk of individuals suffering some harm. Cases must be considered on their own merits and there is no precise rule as to what constitutes a large volume of personal data. Guidance available from http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_7.aspx

Step	Action	Notes
26	Consider, as necessary, the need to notify any third parties who can assist in helping or mitigating the impact on individuals.	E.g. police, insurers, professional bodies, funders, trade unions, website/system owners, bank/credit card companies.
Step	**Action**	**Notes**
D	**Evaluation and Response**	**To evaluate the effectiveness of the School's response to the breach.**
27	Establish where any present or future risks lie.	
28	Consider the data and contexts involved.	E.g. what data is held, its extent, sensitivity, where and how it is stored, how long it is kept.
29	Consider and identify any weak points in existing security measures and procedures.	E.g. in relation to methods of storage and/or transmission, use of storage devices, levels of access, systems/network protections.
30	Consider and identify any weak points in levels of security awareness/training.	Fill any gaps through training or tailored advice.
31	Report on findings and implement recommendations.	Report to Principal/Governance.

Timeline of Incident Management

Date	Time	Activity	Decision	Authority

Appendix 2: Data Protection Request (subject access request)

ACCESS TO PERSONAL DATA PROTECTION REQUEST

(Subject Access Request – SARS)

Enquirer/s Surname:		**Enquirer's Forenames:**	
Enquirer's Address:			
Enquirer's Postcode:		**Enquirer's Tel No:**	
Enquirer's Email:			
Are you the person who is the subject of the records you are enquiring about (i.e. the "Data Subject")?			**YES / NO**
If NO,			
Do you have parental responsibility for a child who is the "Data Subject" of the records you are enquiring about?			**YES / NO**
If YES,			
Name of child or children about whose personal data records you are enquiring			
Description of Concern/Area of Concern			
Description of Information or Topic(s) Requested (In your own words)			

Additional Information	

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

Name

Address

Postcode

DATA SUBJECT DECLARATION

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

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

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

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

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

Dated _____

Appendix 3: Data Protection Impact Assessment (DPIA)

Step 1: identify the need for a DPIA	
Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. *Summarise why you identified the need for a DPIA.*	

This DPIA is considered a 'live' document. This means that it is subject to regular review or re-assessment should the nature, scope, context or purpose of the processing alter for any reason.

Step 2: describe the data processing in more detail	
Nature of the data processing	
How will you collect, use, store and delete the data?	
What is the source of the data?	
Will you be sharing the data with anyone?	
What types of processing are involved that can be identified as potentially high risk?	
Scope	
What is the nature of the data, and does it include special category or criminal offence data?	
How much data will you be collecting and using?	
How often?	
How long will you keep it?	
How many individuals are affected?	
Context	
What is the nature of your relationship with the individuals?	
Do they include children or other vulnerable groups?	
How much control will they have over the processing?	
Would they expect you to use their data in this way?	

Have there been prior concerns or previous security flaws to do with this type of processing?	
Is it novel in any way?	
What is the current state of technology in this area and are there any current issues of public concern that you should factor in?	
Purposes	
What do you want to achieve?	
What is the intended effect on individuals?	
What are the benefits of the processing for you, and more broadly?	

Step 3: consultation process	
Explain how you will consult with relevant stakeholders	
When and how will you seek individuals' views on your data processing activity?	
If you feel it's not appropriate to consult with relevant stakeholders, how can you justify this decision? (Make sure you always record any decision not to consult)	
If you are consulting, who else within your organisation do you need to involve?	
Do you need any of your data processors or any other third parties to help with the consultation?	
Do you plan to consult information security experts, or any other experts?	

Step 4: assess necessity and proportionality	
Describe how you will make sure you comply with data protection law, and keep the processing proportionate to what you actually need	
What is your lawful basis for processing the data in this way?	
Does the processing actually achieve your purpose?	
Is there a less intrusive way to achieve the same outcome?	
How will you ensure the data is good quality and limited to what is necessary?	
What information will you give individuals about how their data is used?	
How will you help to support their rights under the GDPR?	
What measures do you take to ensure processors and other third parties comply with data protection law?	
How do you safeguard any international transfers of the data?	

Step 5: identify and assess risks			
Describe the source of risk and the nature of potential impact on individuals	Likelihood of harm	Severity of harm	Overall risk
Risks may include: • *A privacy breach caused by technical issues or human error, where individuals are at risk of discrimination, identity theft, fraud, loss of confidentiality, physical or emotional harm* • *school*			
Poor processes or inadequate due diligence leading to non-compliance with the GDPR, resulting in financial or reputational damage to the school			
• *Cyber security for parents*			
• *External providers, welfare checks etc. all now working from home*			

Step 6: identify measures to reduce risk				
For risks identified as medium or high, identify additional measures you will take to reduce or eliminate the risk				
Risk	**Options to reduce or eliminate risk**	**Effect on risk *(eliminated, reduced or accepted)***	**Residual risk *(low, medium or high)***	**Measure approved *(yes or no)***

Step 7: sign off and record outcomes		
	Name and date	**Actions**
Measures approved by:		
Residual risks approved by:		
DPO advice provided:		
Summary of DPO advice:		
DPO advice accepted or overruled by:		
If the advice was overruled, explain why:		
Consultation responses reviewed by:		
If your decision is not the same as individuals' views, explain why, and why you have decided to continue with the processing:		
This DPIA will be kept under review by (name):		
Date:		

Appendix 4: Retention Schedule

Type of Record/Document	Suggested Retention Period
SCHOOL-SPECIFIC RECORDS	
Registration documents of School	Permanent (or until closure of the school)
Attendance Register	6 years from last date of entry, then archive
Minutes of Governors' meetings	6 years from date of meeting
Annual curriculum	From end of year: 3 years (or 1 year for other class records: eg marks/timetables/assignments)
INDIVIDUAL PUPIL RECORDS	***NB - this will generally be personal data***
Admissions: application forms, assessments, records of decisions	25 years from date of birth (or, if pupil not admitted, up to6 months from that decision).
Examination results (external or internal)	7 years from pupil leaving school
Pupil file including: o Pupil reports o Pupil performance records o Pupil medical records	ALL: 25 years from **date of birth*** **unless there is good reason to consider this may be applicable evidence in a medical negligence or abuse claim:* see 'Safeguarding' below.
Special educational needs records *(to be risk assessed individually)*	Date of birth plus up to 35years (allowing for special extensions to statutory limitation period)
SAFEGUARDING	
Policies and procedures	Keep a permanent record of historic policies
DBS disclosure certificates (potentially sensitive personal data & must be secure)	No longer than 6 months from **decision** on recruitment itself
Incident reporting	Keep on record for 25 years, ideally reviewed regularly (eg every 6 years)
CORPORATE RECORDS (where applicable)	***Eg. where schools have trading arms***
Certificates of Incorporation	Permanent (or until dissolution of the company)
Minutes, Notes and Resolutions of Boards or Management Meetings	Minimum - 10 years
Shareholder resolutions	Minimum - 10 years
Register of Members/Shareholders	Permanent (minimum 10 years for ex members/ shareholders)
Annual reports	Minimum - 6 years
ACCOUNTING RECORDS	
Accounting records *(normally taken to mean records which enable a company's accurate financial position to be ascertained & which give a true and/air view of the company's financial state)*	Minimum - 6 years for UK charities (and public companies) from the end of the financial year in which the transaction took place Internationally: can be up to 20 years depending on local legal/accountancy requirements
Tax returns	Minimum - 6 years
VAT returns	Minimum - 6 years

Budget and internal financial reports	Minimum - 6 years
CONTRACTS AND AGREEMENTS	
Signed or final/concluded agreements *(plus any signed or final/concluded variations or amendments)*	Minimum - 7 years from completion of contractual obligations or term of agreement, whichever is the later
Deeds (or contracts under seal)	Minimum - 13 years from completion of contractual obligation or term of agreement
INTELLECTUAL PROPERTY RECORDS	
Formal documents of title (trade mark or registered design certificates; patent or utility model certificates)	Permanent (in the case of any right which can be permanently extended, eg. trade marks); otherwise expire of right plus minimum of 7 years.
Assignments of intellectual property to or from the school	As above in relation to contracts (7 years) or, where applicable, deeds (13 years).
IP/IT agreements (including software licences and ancillary agreements eg maintenance; storage; development; co-existence agreements; consents)	Minimum - 7 years from completion of contractual obligation concerned or term of agreement
EMPLOYEE/ PERSONNEL RECORDS	
Contracts of employment	Minimum - 7 years from effective date of end of contract
Employee appraisals or reviews and staff personnel file	Duration of employment plus minimum of 7 years
Payroll, salary, maternity pay records	Minimum - 6 years
Pension or other benefit schedule records	Possibly permanent, depending on nature of scheme
Job application and interview/rejection records (unsuccessful applicants)	Minimum - 3 years (but see note of DBS disclosure certificates above)
Immigration records	Minimum - 4 years
Health records relating to employees	Minimum of 7 years from end of contract of employment
INSURANCE RECORDS	
Insurance policies (will vary - private, public, professional indemnity)	Duration of policy (or as required by policy) plus a period for any run-off arrangement and coverage of insured risks: ideally, until it is possible to calculate that no living person could make a claim.
Correspondence related to claims/ renewals/notification re: insurance	Minimum - 7 years
ENVIRONMENTAL & HEALTH RECORDS	
Maintenance logs	10 years from date of last entry
Accidents to children	25 years from birth (unless safeguarding incident)
Accident at work records (staff)	Minimum - 4 years from date of accident, but review case-by-case where possible
Staff use of hazardous substances	Minimum - 7 years from end of date of use
Risk assessments (carried out in respect of above)	7 years from completion of relevant project, incident, event or activity