METHERINGHAM PRIMARY SCHOOL

METHERINGHAM PRIMARY SCHOOL

Policies, Procedures, Regulations and Guidance

Document Title:	GDPR Policy
Date Effective From:	May 2026
Date of Last Review:	May 2025
Date of Next Review:	May 2027
Approved by:	

Version Control Table *[To be updated as required]*

Version Number	Date Authorised	Summary of Key Changes
2	Take this out, and just leave in the paragraph at Section 14	Updates in line with new Data (Use and Access) act 2025, that came into force in February 2026, mainly affecting: • 2. Legislation guidance • 3. Definitions • 6. Data protection principles • 7. Collection personal data • 8. Sharing personal data • 9. Subject access request (specifically, timelines)

		• 14. Artificial Intelligence • Additional section 19: Data protection complaints

Contents

1. Aims 3
2. Legislation and guidance 3
3. Definitions 3
4. The data controller 5
5. Roles and responsibilities 5
6. Data protection principles 6
7. Collecting personal data 6
8. Sharing personal data 8
9. Subject access requests and other rights of individuals 9
10. Parental requests to see the educational record 12
13. Photographs and videos 12
14. Artificial intelligence (AI) 13
15. Data protection by design and default 13
16. Data security and storage of records 14
17. Disposal of records 14
18. Personal data breaches 14
19. Data Protection Complaints 15
20. Training 16
21. Monitoring arrangements 16
22. Links with other policies 16
Appendix 1: Personal data breach procedure 17
Appendix 2: Data Breach Record 19
Appendix 3: Internal Subject Access Request form 21
Appendix 4: External Subject Access Request Form 25

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents and carers, 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)
- Data (Use and Access) Act 2025

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

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.

TERM	DEFINITION
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 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.
Recognised Legitimate Interests	A legal reason that allows the school to use personal information without asking for consent, when this is necessary to keep people safe, prevent harm or crime, respond to emergencies, or support public services such as safeguarding children.
Automated Decision-Making (ADM) (including "solely automated")	The processing of personal data using automated means, without any human involvement, to make a decision about an individual that has legal effects or similarly significant effects on them. Solely automated decision-making refers specifically to decisions that are made entirely by an automated system, with no meaningful human review or intervention at the point the decision is made.

TERM	DEFINITION
Data Protection Complaint	A concern raised by an individual about how their personal information has been used or handled by the school.
Relevant Time Period (for SARs)	The time period within which an organisation must respond to a subject access request under data protection law. This period does not begin until the school has received sufficient information to confirm the requester's identity and, where reasonably required, clarification of the request. The response period may be paused ("stopped") while awaiting this information and resumes once it has been received. If the person requestion the SAR is unhappy with the response, they can exercise their right to complain to the DPO in the first instance. If there is no satisfactory response, then a complaint can be made to the ICO
Broad Consent	Permission given for personal information to be used for a general type of research, rather than one specific study. This type of consent can be withdrawn at any time. In schools, this is rarely used and would usually apply only to approved educational research

4. The data controller

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

The school has paid its data protection fee to the ICO, 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 Governing board

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

5.2 Data protection officer (DPO)

The data protection officer (DPO) 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 governing board and, where relevant, report to the board their 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.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Judy Carter and is contactable via 07834 690 101.

5.3 Headteacher

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

5.4 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 DPO 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 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

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 1 of 7 '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**
- Recognised Legitimate Interests – the data needs to be processed for certain recognised purposes set out in legislation, where the processing is necessary and no balancing test is required.

  These purposes include, but are not limited to:

  - safeguarding children and vulnerable individuals
  - preventing, detecting or investigating crime
  - responding to emergencies
  - supporting public authorities in carrying out their statutory functions

For special categories of personal data, we will also meet 1 of the special category conditions for processing under data protection law:

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

- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

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

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

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. However, there are circumstances where we may need to share personal data **without consent**, where this is lawful and necessary. These circumstances include, but are not limited to, situations where:

- There is a concern relating to a pupil or parent/carer that may affect the safety or wellbeing of pupils or staff
- We need to share information with other agencies or professionals to support children, families or staff, including for safeguarding purposes
- We are required to share information to comply with a legal obligation or to support law enforcement or regulatory bodies
- We need to respond to an emergency situation involving pupils or staff

Where appropriate, we will share personal data with:

- Local authorities

- Emergency services
- Health professionals
- Law enforcement and government bodies
- Other schools or educational settings
- Suppliers, contractors or professional advisers acting on the school's behalf

8.1 Sharing data with suppliers and contractors

Where we share personal data with suppliers or contractors (for example, IT service providers, software platforms or external professionals), we will:

- Only appoint organisations that can provide sufficient guarantees that they comply with UK data protection law
- Put a written contract or data processing agreement in place which sets out:
    - how the personal data may be used
    - how it must be kept secure
    - the supplier's responsibilities and obligations
- Only share the minimum amount of personal data necessary for the supplier to provide the service

8.2 International transfers of personal data

In some cases, the school may need to share or store personal data outside the United Kingdom, for example where a supplier uses cloud-based systems hosted overseas.

Where personal data is transferred outside the UK, we will ensure that the transfer is carried out in accordance with UK data protection law and that appropriate safeguards are in place.

These safeguards may include:

- Transferring data to countries that have been confirmed by the UK government as providing an adequate level of data protection
- Using the International Data Transfer Agreement (IDTA) approved for use in the UK
- Using the UK Addendum to the EU Standard Contractual Clauses, where applicable
- Carrying out appropriate risk assessments and applying additional security measures where needed

We will not transfer personal data internationally unless we are satisfied that individuals' rights and freedoms are adequately protected.

Information about any international data transfers will be included in the school's relevant privacy notices.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a '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
- Subject access requests can be made by submitting the form in appendix 4 to the headteacher

If staff receive a subject access request in any form they must immediately forward it to the DPO, using the form in appendix 3

9.2 Children and subject access requests

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

There is no fixed age at which a child is considered capable, however, 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.

9.3 Responding to subject access requests

When responding to subject access requests, we will:

- Take reasonable steps to verify the identity of the individual making the request. This may include asking for up to two forms of identification, where necessary
- Contact the individual, where appropriate, to clarify the scope of their request so that we can respond accurately and efficiently

Timescales

We will respond to a subject access request without undue delay and within one month of the relevant time period starting.

The relevant time period does not begin until:

- We have received sufficient information to confirm the requester's identity, and
- We have received any clarification needed to understand the request

Where we are awaiting identity confirmation or clarification, the response timescale may be paused ("stopped") and will resume once the required information has been provided.

Where a request is complex or where we have received a number of requests from the same individual, we may extend the response period by up to a further two months.

If this applies, we will:

- Inform the individual within one month, and
- Explain why the extension is necessary

Providing the information

- We will normally provide the requested information free of charge
- We will carry out reasonable and proportionate searches for personal data in response to the request

If the request is manifestly unfounded or excessive, we may:

- refuse to act on it, or
- charge a reasonable fee to cover administrative costs

Exemptions and refusals

We may withhold or restrict access to information where disclosure is permitted to be limited by data protection law, including where the information:

- Could cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal information about abuse or safeguarding concerns where disclosure would not be in the child's best interests
- Includes personal data about another individual that cannot reasonably be anonymised and where consent has not been given
- Is subject to legal privilege or forms part of certain confidential or sensitive records, such as:
    - crime or law enforcement records
    - immigration records
    - legal proceedings or legal advice
    - confidential references or exam scripts

Where we refuse a request or withhold information, we will:

- Explain the reason for our decision, and
- Inform the individual of their right to complain to the Information Commissioner's Office (ICO) and to seek enforcement through the courts

9.4 Other data protection rights of the individual

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

- Withdraw their consent to processing at any time, where consent is the lawful basis
- Ask us to rectify inaccurate personal data
- Ask us to erase personal data or restrict its processing, in certain circumstances
- Object to processing that is carried out on the basis of public task, legitimate interests, or recognised legitimate interests
- Prevent the use of their personal data for direct marketing purposes
- Challenge decisions that are based solely on automated processing, where those decisions have legal effects or similarly significant effects on them
- Request meaningful human intervention, express their view, and contest such decisions where automated decision-making is used
- Be notified of a personal data breach, where required by law
- Make a complaint to the school or to the Information Commissioner's Office (ICO)
- Request that their personal data be transferred to another organisation in a structured, commonly used and machine-readable format, where applicable

Where the school uses automated processing to support decision-making, we will ensure that appropriate safeguards are in place, including transparency about how decisions are made and access to human review where required.

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.

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.

13. 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 the 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.

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.

14. Artificial intelligence (AI)

Artificial intelligence (AI) and automated systems are increasingly used in education, including for administrative tasks, learning support, monitoring systems and data analysis. The school recognises that while AI and automated tools may offer benefits, they also present risks to personal data and individual rights. Further guidance on acceptable use of AI is set out in the school's AI policy and Acceptable Use Policy.

15. 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 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 DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may 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 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, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

16. 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, 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
- 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
- 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)

17. Disposal of records

Personal data that is no longer needed will be disposed of securely in line with IRMS 2924 Recommendations for Schools. 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.

18. 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

19. Data Protection Complaints

Individuals have the right to make a complaint directly to the school if they are concerned about how their personal data has been collected, used, shared, stored, or otherwise processed, or if they believe their data protection rights have not been respected.

19.1 How to make a data protection complaint

Data protection complaints may be made in writing to the school using any of the following methods and sent via:

- email: enquiries@metheringham.lincs.sch.uk
- post:

  Metheringham Primary School

  Princes Street

  Metheringham

  Lincoln

  LN4 3BX

Complaints should clearly explain the concern and, where possible, include relevant details to help us investigate the matter.

19.2 Handling of data protection complaints

All data protection complaints will be handled by the school's Data Protection Officer (DPO), Judy Carter

The school will:

- Acknowledge receipt of the complaint
- Investigate the complaint fairly and thoroughly
- Respond without undue delay and in accordance with data protection law

Where necessary, we may contact the complainant to seek further information or clarification in order to resolve the complaint appropriately.

19.3 Right to escalate a complaint

If an individual is unhappy with the school's response to a data protection complaint, they have the right to escalate the matter to the Information Commissioner's Office (ICO), the UK's independent regulator for data protection:

Information Commissioner's Office (ICO)

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Tel: 0303 123 1113

Website: https://www.ico.org.uk

Individuals also retain the right to seek enforcement of their data protection rights through the courts.

20. Training

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

21. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the full governing board.

22. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO) by completing the data breach form in appendix 2.
- 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
- Staff and governors will co-operate 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 DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types 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) before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
- The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in 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, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. 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 of the school's awareness of the breach. 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
- 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 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 in the schools' computer system (Virtual Staffroom / Documents / GDPR)
- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible
- The DPO and headteacher will meet annually to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Appendix 2: Data Breach Record

METHERINGHAM PRIMARY SCHOOL: DATA BREACH RECORD

Date of breach:					
Person responsible for dealing with breach?					
Reported by:					
Date investigation started:					
Date investigation completed:					
Description and nature of the breach:					
Number of data subjects involved:					
Data type involved:					
Phone/email sent to DPO?	Yes/No	Is this high risk?	Yes/No	Report to ICO?	Yes/No
Date reported to data subjects:					
Actions taken:					
Preventative action suggestions and risks as a result of the breach (including training)					
Notes					

Actions approved by DPO		Date	/ /

DATA BREACHES

- GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible. However, it is not always possible to investigate a breach fully within 72 hours to understand fully what has happened. You are allowed to provide the required information in phases, as long as this is done without undue further delay, and the breach has been notified (but investigation of the breach should be prioritised).
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.
- You should ensure you have robust breach detection, investigation and internal reporting procedures in please. This will facilitate decision making about whether or not you need to notify the relevant supervisory authority and the affected individuals.
- You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. There will be a personal data breach whenever any personal data is lost, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Personal data breaches can include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controlled or processor
- Sending personal data to an incorrect recipient
- Computing devises containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

Reporting a Data Breach

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. This should be discussed with your DPO as soon as possible. If it's likely that there will be a risk then the ICO must be notified; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should record it.

Appendix 3: Internal Subject Access Request form

The below form should be completed by the school and submitted to the DPO as soon as a subject access request is received

METHERINGHAM PRIMARY SCHOOL: SUBJECT ACCESS REQUEST

Name of data subject	
Name of person who made request	
Date request received	
ID of person making request checked	*Indicate type of ID confirmation*
Contact DPO (date)	
Date acknowledgement sent to person making the request	
Name of person dealing with request and position in School	
Is the person entitled to the data?	
Do you understand what data they are asking for?	
Identify the data	
Collect the data required	
Do you own all the data?	
Do you need to exempt/redact data?	
Is the data going to be ready in time?	
Create pack	
Inform requestor you have the data or if you require more time to complete the request	
Deliver data	

Date request completed (within 30 days of request):_____

Signed off by:_____ (Headteacher)

NOTES

1. Subject access request should be made to the school in writing and ID of person making the request confirmed.
2. The school has 30 days to respond to the request.
3. The school should have a standard letter to reply to the request:
    a. Inform them that the school has 30 days to respond
    b. Inform them how the information will be supplied
4. The school has a right to refuse a Subject Access Request – if you do this, then you must state legally why.

Are they entitled to the data?

If no, reply stating your reasons and/or ask for proof.

Do you understand what data they are asking for?

If no, ask requestor for clarity

Identify the data

What are your data sources, and where are they kept

Collect the data required

You may need to ask others – state a deadline to these people in your request

Do you own all the data?

If no, ask third parties to release external data. If data is supplied by another agency (such as the Psychology Service etc) you do not own the data.

Do you need to exempt/redact (edit) the data?

If exempting/redacting, be clear of your reasons. Document name, date exempted/redacted, and why.

Is the data going to be ready in time?

Record delays and reasons. Communicate with requestor stating reason for delay and asking if they would like the data you have collected so far.

Create pack

Make sure that the data is in an easy format to access: paper/Word/Excel etc

Inform requestor you have the data

Ask them how they would like it delivered

Deliver data

Ask for confirmation of delivery – special delivery?

Metheringham Primary School

Subject Access Request – Document List (insert surname of family)

Child: (put first name)		
Document	Location Kept	Redaction Notes
e.g. end of year report 2017	Electronic – staff drive In child's file – filing cabinet	
e.g. end of year report 2018		
e.g. behaviour record	HT office – behaviour file	Pg 1 – name of another child removed

Appendix 4: External Subject Access Request Form

To initiate the subject access request, the below form should be submitted to the headteacher:

Dear Headteacher,

Please provide me with the information about me that I am entitled to under the General Data Protection Regulation. This is so I can be aware of the information you are processing about me, and verify the lawfulness of the processing.

Applicant's Name	
Name of Subject / Adult / Pupil:	
Please note, when searching for data electronically, for instance emails and electronic files, the school will search the term: "subject:"FIRSTNAME" AND subject:"SURNAME"	
Relationship with the School	**Please Select** Pupil / parent / employee / governor / volunteer Other (please specify)
Correspondence address	
Contact Number	
Email Address	
Please bear in mind that under the GDPR there is no fee to provide this information, and in most cases, the information will be supplied within 1 month. However, in cases where the information is complex or involves capturing large volumes of information, the School has the right to extend this deadline by a further two months in accordance with the guidance issued by the Information Commissioner's office. However, if you are able to make your request with precise short timeframes and being specific on the types of records we need to search, and be specific about what information you are seeking, then this may enable the School to provide you with the information more quickly. In line with the Data Use and Access Act (DUAA) (2026), the school is entitled to the "stop the clock" rule, whereby the one-month deadline is paused for genuine need of clarification on a request, resuming only once the information is provided. Below is a list of data we may hold:	
Details of the information requested	**Please provide me with:** Insert details of the information you want that will help us to locate the specific information quickly. Please be as precise as possible, please highlight:

	• School Reports • Attendance information • Dinner orders • Academic data • Registration details • Emails between school and parents • Emails between school and agencies • TAC Meeting Minutes • Child in Need Minutes • Tapestry • SENDCo Files (including electronic) • Meeting minutes • CPOMS Reports (Including Safeguarding records) • Correspondence from parents to enquiries@cranwell.lincs.sch.uk • Correspondence between parents and a staff member (please name the staff member) Other:
Between which dates do you want the information?	Being specific is very important. The shorter the time period, the quicker the search will be.
How would you like to receive the information?	Via secure email or via post?

Please send this completed form to : enquiries@metheringham.lincs.sch.uk FAO: the Headteacher.

If the school require any further information from you they will be in touch as soon as possible.

You have the right to exercise a complaint if you are not happy with the response. Please see the School's GDPR and data protection policy for details on how to do this.

If you need any advice on dealing with this request, you can contact the Information Commissioner's Office on 0303 123 1113 or at www.ico.org.uk