



Newtown C of E Primary School

Data Protection Policy

Ratification Date:	September 2018	Signed:	Mrs Emma Howlett (HEADTEACHER) Mrs Janet Cane (CHAIR OF GOVERNORS)
Reviewed	November 2023	Signed	Mrs Emma Howlett (Headteacher) Mrs Glynis Wright (Chair of Governors)
Reviewed	November 2024	Signed	Mrs Emma Howlett (Headteacher) Mrs Glynis Wright (Chair of Governors)
Reviewed	November 2025	Signed	Mrs Emma Howlett (Headteacher) Mrs Glynis Wright (Chair of Governors)
Next Review	November 2025		

School Vision

At Newtown C of E Primary School, our motto is enriched and sustained by our Christian values of **Love, Courage and Friendship**, rooted in the teachings of the Bible. We are guided by the call to “*love one another as I have loved you*” (John 13:34), “*be strong and courageous... for the Lord your God is with you wherever you go*” (Joshua 1:9), and “*a friend loves at all times*” (Proverbs 17:17).

As a school at the heart of an evolving community, we warmly welcome children and families from a wide range of backgrounds and experiences. We are enriched by the unique qualities each child brings and value the talents and perspectives that help us grow together.

We are an aspirational school serving our community. We seek to know, understand and celebrate every child, nurturing their individual strengths and talents. We prepare our children to become confident, responsible global citizens in an ever-changing world, guided by our core values of love, courage and friendship.

Through **Love**, we show kindness, compassion and generosity, building a community where everyone feels safe, welcomed and valued. Through **Courage**, we persevere, meet challenge with confidence, and stand up for what is right with honesty and grace. Through **Friendship**, we grow together — encouraging one another, celebrating each other’s gifts, and looking to the future with hope and aspiration.

We live out these values by:

- Being a caring, welcoming and inclusive Christian community where staff, pupils, parents and governors work together in a safe and supportive environment, inspired by “*Above all, love each other deeply*” (1 Peter 4:8)
- Promoting the welfare and dignity of every child, safeguarding them from harm — including physical, sexual and emotional abuse, neglect and bullying — in accordance with statutory guidance in *Keeping Children Safe in Education* (Department for Education)
- Providing a rich, engaging curriculum that equips children with the knowledge, skills and character to become lifelong learners and responsible citizens, reflecting Christian teachings and British Values
- Building strong, positive partnerships with parents, the church and the wider community, and encouraging participation in local, national and global initiatives

- Fostering our Learning Behaviours of Resilience, Focus, Independence, Self-Regulation, Respect and Boundaries, encouraging children to act with integrity, perseverance and kindness in all they do

At Newtown, we want every child to know they belong, are cherished, and are capable of great things. Through **Love, Courage and Friendship**, we grow minds, shape futures and journey together in hope.

1. Statement of Intent

Newtown C of E Primary School is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the GDPR.

The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies and potentially children's services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the school complies with the following core principles of the GDPR.

Organisational methods for keeping data secure are imperative and Newtown C of E Primary School believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy complies with the requirements set out in the GDPR, which came into effect on 25 May 2018.

2. Aims

The school collects and uses personal information (referred to in [General Data Protection Regulation \(GDPR\)](#) as personal data. This information is gathered in order to enable the provision of education and other associated functions. In addition, the school may be required by law to collect, use and share certain information.

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 the [General Data Protection Regulation \(GDPR\)](#) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the [Data Protection Bill](#).

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

3. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the [GDPR](#) and the ICO's [code of practice for subject access requests](#). It 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, 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.
ICO	Information Commissioner's Office
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 as a data controller with the ICO and will renew this registration annually or as otherwise legally required. Data Controllers have a general duty of accountability for personal data.

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 body

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

5.2 Data protection officer

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 report 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.

Our DPO is the School Business Manager, and is contactable via the school office or at adminoffice@newtown.sch.uk

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 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 contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on six 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 and not further processed in a manner that is incompatible with those purposes (subject to exceptions for specific archiving purposes)
-  Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed and not excessive
-  Accurate and, where necessary, kept up to date
-  Kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which it is processed
-  Processed in a way that ensures it is appropriately secure

The school is committed to maintaining the principles and duties in the GDPR. **Appendix 1** of this policy sets out how the school aims to comply with these principles.

7. Collecting personal data

7.1 What is Personal Information/data?

Personal information or data means any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified, directly or indirectly, by reference to details such as name, an identification number, location data, an online identifier or by their physical, physiological, genetic, mental, economic, cultural or social identity. Personal data includes (but is not limited to) an individual's name, address, date of birth, photograph, bank details and other information that identifies them.

7.2 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 (GDPR) that must be adhered to at all times:

-  The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
-  The data needs to be processed so that the school can **comply with a legal obligation**
-  The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
-  The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest**, and carry out its official functions
-  The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
-  The individual (or their parent/carers 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 which are set out in the GDPR and Data Protection Act 2018.

Special Category Data is data being used because it is legally necessary and the use of the data is in the “substantial public interest.” This data is kept for 7 years and will be deleted or shredded at the end of this period.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent.

7.3 Limitation, minimisation and accuracy

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

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

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

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Hampshire County Council Retention of Records Policy.

8. Sharing personal data

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

-  There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
-  We need to liaise with other agencies – we will seek consent as necessary before doing this
-  Our suppliers or contractors need data to enable us to provide services to our staff and pupils, for example, IT companies. When doing this, we will:
 - o Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
 - o Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
 - o Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

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

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

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

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law and where that country ensures an adequate level of data protection.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' (SAR) 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
-  The source of the data, if not the individual
-  Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

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

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

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

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.

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 requests, we:

-  May ask the individual to provide 2 forms of identification
-  May contact the individual via phone to confirm the request was made
-  Will respond without delay and within 1 month of receipt of the request
-  Will provide the information free of charge
-  May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and

explain why the extension is necessary

We will not disclose information if it:

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

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

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

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

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
-  Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
-  Prevent use of their personal data for direct marketing
-  Challenge processing which has been justified on the basis of public interest
-  Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
-  Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
-  Prevent processing that is likely to cause damage or distress
-  Be notified of a data breach in certain circumstances
-  Make a complaint to the ICO
-  Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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

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.

11. 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. This is done at the time of admission to the school. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. A list of children who may not be photographed or filmed is kept in the school office. It is good practice for staff to check whether consent has been provided when there is a chance that photographs or filming may take place.

Uses may include:

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

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

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

See our E-Safety and Rules for the Use of ICT Policy for more information on our use of photographs and videos.

12. 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 and time to fulfil their duties and maintain their expert knowledge
-  Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
-  Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
-  Integrating data protection into internal documents including this policy, any related policies and privacy notices
-  Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
-  Regularly conducting reviews to monitor our privacy measures and make sure we are compliant
-  Maintaining records of our processing activities, including:
 - o 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)
 - o For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data

secure

13. 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. Laptops and paper-based data will be kept secure when being transported by being kept in a lockable bag or trolley. Computer and laptop screens must be locked when staff away from their desks. iPads must be secured.
-  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 public access
-  Where personal information needs to be taken off site, away from their personal home, staff must sign it in and out from the school office e.g. pupil and emergency contact details for residential and day trips.
-  Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
-  Encryption software is used to protect all portable devices and removable media, such as USB devices. Staff **MUST ONLY** use their encrypted memory stick or work via the remote portal when offsite, to save and transfer documents.
-  Staff, pupils or governors **MUST NOT** store school information on any personal devices e.g. own personal laptop. Staff may use a personal laptop but can only work through the remote portal and **MUST NOT** store school data to their own personal hard-drive.
-  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)

14. 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.

15. 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 2.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school

context may include, but are not limited to:

-  A non-anonymised dataset being published on the school website which shows the exam results of 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

16. Training

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

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

17. Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to the handling of personal information may be referred to the Information Commissioner (ICO) who can be contacted at:

Wycliffe House Water
Lane Wilmslow Cheshire
SK9 5AF
Or at www.ico.gov.uk

18. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

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

19. Links with other policies

This data protection policy is linked to our:

-  E-Safety & Rules for the Use of ICT policy
-  Child protection policy
-  Safeguarding Policy

Appendix 1: The School Commitment

The school is committed to maintaining the principles and duties in the GDPR at all times.

Therefore, the school will:

-  Inform individuals of the identity and contact details of the data controller
-  Inform individuals of the contact details of the Data Protection Officer.
-  Inform individuals of the purposes that personal information is being collected and the basis for this
-  Inform individuals when their information is shared, and why and with whom unless the GDPR provides a reason not to do this.
-  If the school plans to transfer personal data outside the EEA the school will inform individuals and provided them with details of where they can obtain details of the safeguards for that information.
-  Inform individuals of their data subject rights.
-  Inform individuals that the individual may withdraw consent (where relevant) and that if consent is withdrawn that the school will cease processing their data although that will not affect the legality of data processed up until that point.
-  Provide details of the length of time an individual's data will be kept.
-  Should the school decide to use an individual's personal data for a different reason to that for which it was originally collected the school shall inform the individual and where necessary seek consent.
-  Check the accuracy of the information it holds and review it at regular intervals.
-  Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in.
-  Ensure that clear and robust safeguards are in place to ensure personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
-  Ensure that personal information is not retained longer than it is needed.
-  Ensure that when information is destroyed that it is done so appropriately and securely.
-  Share personal information with others only when it is legally appropriate to do so.
-  Comply with the duty to respond to requests for personal information (known as Subject Access Requests)
-  Ensure that personal information is not transferred outside the EEA without the appropriate safeguards.
-  Ensure that all staff and governors are aware of and understand these policies and procedures.

Appendix 2: Personal data breach procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

-  On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.
-  The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
 - Lost
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been
 - Made available to unauthorised people
-  The DPO will alert the Headteacher and the Chair of Governors
-  The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
-  The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
-  The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
 - Loss of control over their data
 - Discrimination
 - Identify theft or fraud or Financial loss
 - Unauthorised reversal of pseudonymisation (for example, key-coding)
 - Damage to reputation
 - Loss of confidentiality
 - Any other significant economic or social disadvantage to the individual(s) concerned

If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

-  The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system in ADMIN/GDPR
-  Where the ICO must be notified, the DPO will do this via the ['report a breach' page of the ICO website](#) within 72 hours. As required, the DPO will set out:
 - A description of the nature of the personal data breach including, where possible:
 - The categories and approximate number of individuals concerned
 - The categories and approximate number of personal data records concerned
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

-  If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
-  The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
-  The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
-  The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - Facts and cause
 - Effects
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the school's computer system in ADMIN.

The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

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

Sensitive information being disclosed via email (including safeguarding records)

-  *If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error*
-  *Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error*
-  *If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT service provider to recall it*
-  *In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way*
-  *The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request*
-  *The DPO will carry out an internet search to check that the information has not been made*

public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Other types of breach 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*
-  *Parental details such as contact details and email addresses being breached*