Date Adopted: **Autumn 2025**
Date to be reviewed: **Autumn 2026**

Quadring Cowley and Brown's Primary School

Data Protection Policy (GDPR)

At Quadring Cowley &Brown's Primary School we strive
'to nurture and inspire all children to be well-rounded, confident and resilient individuals who love learning and are ready for life beyond school.'

Article 3- The best interests of the child must be top priority in all actions regarding children.
Article 36- Children must be protected from things that could harm them

Intent of the Policy
Quadring Cowley and Brown's Primary School is committed to and aims to ensure that all personal data collected about staff, pupils, parents, school Governors, visitors and other individuals who come into contact with the school is collected, stored and processed in accordance with data protection legislation including the UK General Data Protection Regulation (GDPR) 2018.
This information is processed in order to enable the School to provide education and other associated functions. In addition, there may be a legal requirement for the School to process personal information to ensure that it complies with statutory obligations.
This policy applies to all personal data, regardless of whether it is in paper or electronic format. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

Scope of the policy
This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the GDPR and DPA and other related legislation. It will apply to personal information regardless of the way it is collected, used, recorded, stored and destroyed and irrespective of whether it is held in paper files or electronically.

The Information Policy applies to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper;
- Information or data stored electronically, including scanned images;
- Communications sent by post/courier or using electronic means such as email or electronic file transfer;
- Information or data stored on or transferred to removable media such as USB storage device or memory card;
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops;
- Speech, voice recordings and verbal communications, including voicemail;
- Published web content, for example intranet and internet;
- Photographs and other digital images.

Quadring Cowley and Brown's Primary School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with it's statutory obligations.

Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Schools also have a duty to issue a Fair Processing Notice to all pupils/parents, this summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

What is Personal Information?
Personal information or data is defined as data which relates to a living individual who can be

identified from that data, or other information held.

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

The principles say that personal data must be:

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

This policy sets out how the school aims to comply with these principles.

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 GDPR .

This policy meets the requirements of the Protection of Freedoms Act 2012 if referring to use of biometric data. However we do not use biometric data as part of our school policy at this time. Introduction of such data collection methods would require approval by the governing body and this policy would be updated to reflect that change.

This policy also reflects the ICO's code of conduct 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.

Definitions

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 individuals: • 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.

The Data Controller

Quadring Primary processes personal data relating to parents, pupils, staff, school Governors, visitors and others, and therefore is a data controller.

The School, as a data controller, is registered with the Information Commissioner's Office (ICO) and pays an annual fee to the ICO. This fee includes all schools (schools do not have separate ICO registration).

Roles and Responsibilities

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

Governing Board

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

Data Controller

The member of staff responsible for data protection, the Data Controller, is the Headteacher, Mrs Jeanette Jameson. The Headteacher may delegate data controller duties as necessary.

The Data Controller is the person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed.

Data Protection Officer
The Data Protection Officer (DPO) at Quadring Primary is Mrs Jane Devine, who can be contacted via the main school office on 01775 820302.

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

The DPO is responsible for monitoring all internal compliance and informs and advises the school about their data protection obligations.

The DPO is responsible for ensuring that all an ongoing program of relevant training, support and information is shared with the relevant persons.

The DPO is also responsible for reporting serious breaches in line with the data protection breach protocol (see Appendix 1) and monitoring and supporting with data Subject Access Requests (SARs).

All data breaches reported to the ICO are also recorded on the Serious Incident Report which is shared with the Headteacher and Governing Board. The DPO is also the first point of contact for the ICO.

The DPO cannot hold a position that requires them to determine the purpose and means of processing personal data, e.g. the Headteacher.

All staff and Volunteers
Staff and volunteers are responsible for:

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

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 processes
- processed in a way that ensures it is appropriately secure.
-

This policy sets out how Quadring Primary School aims to comply with these principles.

Collecting Personal Data

1. **Lawfulness, fairness and transparency**

We will only process personal data where we have one of six 'lawful bases' (legal reasons) to do so under UK data protection law:
• The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering 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 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 or exercise its official authority.
• The data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden).
• The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out under UK 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 UK 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.

Further information is available within our suite of Privacy Notices, on the school website.

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 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 retaining records policy.

3. 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 UK 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, 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.

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

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

Data Protection Impact Statements
The school will evidence the thought and decision-making process about data protection when designing any processes in school which involve personal data.
A Data protection Impact Statement (DPIA) is needed when:
- New technology is being deployed
- A profiling operation is likely to significantly affect individuals
- There is processing on a large scale of the special categories of data as specified in the GDPR Guidance.

Subject Access Requests and other rights of individuals
Subject Access Requests (SAR)
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 is not 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.
• 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 safeguards provided if the data is being transferred internationally.
Subject access requests may be submitted in any form, but we may be able to respond more quickly if they are submitted in writing, either by letter or email, to the school 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 school Data Protection Officer. The DPO keeps a register of all data subject access requests in a Data Protection Log.

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, subject access requests from parents or carers of pupils below the age of 12 will usually be granted without the express permission of the pupil. Most subject access requests from parents or carers of pupils aged 12 or older will 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.

Responding to subject access requests
When responding to requests:
• We may ask the individual to provide two forms of identification.
• We may contact the individual via phone to confirm the request was made.
• We will respond without delay and within one month of receipt of the request (or receipt of the additional information needed to confirm identity or consent, where relevant)
• We may tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month and explain why the extension is necessary.
• We will provide the information free of charge.

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 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 cannot reasonably anonymise, and we do not 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.

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 or they can seek to enforce their subject access right through the courts.

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 Sharing personal data), 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 school Data Protection Officer. If staff receive such a request, they must immediately forward it to the DPO.

Parental Requests to see the educational record of their child
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 days of receipt of a written request.

CCTV
If CCTV is used around the school to ensure the sites 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 use of CCTV system should be directed to the relevant school DPO.

Photographs and videos
As part of school activities, we may take photographs and record images of individuals within our schools.

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 do not need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

When the school takes photos or videos, uses may include:
• Within schools 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 websites 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 as soon as is reasonably practicable.

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.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by UK data protection legislation. We will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, and we will ask for parents/carers to sign a memorandum of understanding at each event, that any breaches of sharing of photographs and videos may lead to further investigation and reporting. Any parents/carers who personally agree with other parents/carers to share photographs or videos of their child/children do so at their own risk and are responsible for this. The school will not be held responsible for any such agreements.

Biometric Data
If the School uses or intends to use biometric data (such as fingerprint technology) a separate, detailed notice will be sent to all pupils and parents explaining the intended reasons for and lawful basis for the use of the data, and provide parents with options for alternative systems if they do not wish their child to provide this information and want to opt out.

The School will obtain the written consent of at least one parent or carer with Parental Responsibility for the child before taking and using any biometric data from a pupil.

Data Protection by Design and Default
We have 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.
• Ensuring that the DPO and relevant Data protection collectors are provided with an ongoing program of training, support and resources.
• Rolling out data protection training and updates for all staff and Governors in response to changing data protection legislation.

• Completing a data protection audit and putting in place a system to keep these updated and maintained.
• 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 UK data protection law.
• Completing Data Protection Impact Assessments (DPIA) 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 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 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.

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 relevant school office. This must only be in exceptional circumstances.
- Passwords that are containing letters and numbers and any other characters are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals and 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 agreement on acceptable use).
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

Disposal of Records
Personal data that is no longer needed will be disposed of securely in line with our Retaining Records Policy. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.
For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with UK data protection law.
The Governing Board will ensure that the school has an up to date and accurate retention and disposal schedule that is compliant with GDPR. The school will ensure that personal data is stored, transferred and disposed of securely and in accordance with the retention and disposal schedule.

Personal Data Breaches
We will make all reasonable endeavours to ensure that there are no personal data breaches.
In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1 and 2.

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 assessment results of pupils
• safeguarding information being made available to an unauthorised person
• the theft of a school laptop containing non-encrypted personal data about pupils

Training
All staff and Governors are provided with data protection training as part of their induction process.
Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

Monitoring Arrangements
The Headteacher and DPO are responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and updated as necessary and shared with the Governing Board.

The Data protection Policy should be read in conjunction with:

- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- Parents, Visitors and Volunteers Code of Conduct
- Governors Code of Conduct
- Acceptable Usage Agreement
- Child Protection and Safeguarding Policy
- Commitment to Confidentiality Statement

- E Safety Policy
- Privacy Notices
-

Further information can be found at:
https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted Data Protection Act 2018

https://www.gov.uk/government/publications/data-protection-toolkit-for-schools
Data Protection Guidance for Schools

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 data protection breach, or potential breach, the staff member or data processor must immediately notify the relevant school Data Protection Officer (see Appendix 2),
- The school DPO will initially investigate the report and 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.

- Where it is clear after an investigation that there has been no breach, the report and outcome of the investigation will be recorded but no further action will be taken.
- Where the school data protection officer finds that there has been a breach, or a potential breach, he or she will report this to 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 nonmaterial damage (e.g. emotional distress), including through:

- loss of control over their data
- discrimination
- identify theft or fraud
- financial loss
- unauthorised reversal of pseudonymisation (for example, key-coding)
- damage to reputation
- loss of confidentiality
- any other significant economic or social disadvantage to the individual(s) concerned.

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

The DPO may also use the ICO's self-assessment tool on the ICO website or call the ICO breach helpline to decide whether a breach is reportable.

• The DPO will document the decision on whether to report to the ICO (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 electronically.

- 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.

- Where the DPO finds there has been a reportable breach, the DPO will alert the Headteacher.
- 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 decide whether to notify third parties/which third parties to notify based on the DPO's investigation and engagement with affected individuals.
- The DPO will also ensure any other relevant parties are notified as required such as the EFSA and Ofsted.
- The Deputy DPO and school data protection lead will document each breach, irrespective of whether it is reported to the ICO, in the Data Protection log. 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 electronically.

- For all breaches, the Headteacher and Data Protection Officer will review what happened and put in place changes to help avoid a recurrence.
- For reportable breaches, the DPO and the Headteacher will review what happened and how it can be stopped from happening again. This will happen as soon as reasonably possible.
- All reportable breaches are recorded by the DPO in the Serious Incident Report and shared with the Governing Board.

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

Sensitive information being disclosed via email (including safeguarding records)
- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT providers 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

Sensitive information being disclosed via school website
- Member of staff who discovers the sensitive information to inform the DPO as soon as possible.
- DPO to arrange for information to be removed from the school website immediately.
- Parents to be informed that sensitive information was available on the website and that action has been taken to remove it.
- DPO to follow data breach protocols.

Appendix 2: Information Security Incident Reporting Timeline of Actions

This guidance has been written to inform employees what to do if they discover an information security incident.

Queries about any aspect of Quadring Primary School's GDPR strategy or corresponding policies should be directed to the Data Protection Officer at the school.

This policy applies to all employees, any authorised agents working on behalf of Quadring Primary School, including temporary or agency staff, elected members, and third party contractors.

Individuals who are found to knowingly or recklessly infringe this policy may face disciplinary action.
They apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper;
- Information or data stored electronically, including scanned images;
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;
- Information or data stored on or transferred to removable media such as USB storage device or memory card;
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops;
- Speech, voice recordings and verbal communications, including voicemail;
- Published web content, for example intranet and internet;
- Photographs and other digital images.

Notification and Containment
Article 33 of the GDPR compels data controllers to report breaches of personal data, to the Information Commissioner's Officer, within 72 hours of discovery, if the incident is likely to result in a risk to the rights and freedoms of data subjects. Therefore it is vital that Quadring Primary School has a robust system in place to manage, contain, and report such incidents.
Immediate Actions (Within 24 Hours)

If an employee, governor, or contractor is made aware of an actual data breach, or an information security event (a 'near-miss'), they must report it to their line manager and the DPO within 24 hours. If the DPO is not at work at the time of the notification then it must be reported to the Headteacher to start the investigation process.

If appropriate, the officer who located the breach, or their line manager, will make every effort to retrieve the information and/or ensure recipient parties do not possess a copy of the information.

Assigning Investigation (Within 48 Hours)
Once received, the Headteacher and DPO will assess the data protection risks and assign a severity rating according to the identified risks and mitigations.
The severity ratings are:

The DPO will recommend immediate actions that need to take place to contain the incident. The Headteacher and DPO will ascertain the severity of the risk and actions will be taken according to the severity rating.

White	Information security event No breach has taken place but there is a failure of the implemented safeguards that could cause a data breach in the future.
Green	Low Risk/Minimal Impact A data breach has occurred but has been contained within the organisation and the information is not considered to be particularly sensitive, and no further action is deemed necessary
Amber	Medium Risk/Moderate Impact Security measures have failed and consequently have resulted in the loss, release, or corruption of personal data. However, the actual or potential detriment is limited in impact and does not reach the threshold for reporting to the information commissioner's office
Red	High Risk/Serious Impact A breach of security involving sensitive personal data and/or a large volume of personal data. The incident has or is likely to cause serious detriment (emotional, financial, or physical damage) to individuals concerned. The breach warrants potential reporting to the information commissioner's office and urgent remedial action. HR input may also be required

Red incidents will be investigated by the Data Protection Officer with the assistance of Internal Audit and Counter Fraud Teams.

Reporting to the ICO/Data Subjects (Within 72 Hours)
The DPO will make a decision as to whether the incident needs to be reporting to the ICO, and also whether any data subjects need to be informed.

Investigating and Concluding Incidents
The DPO will ensure that all investigations have identified all potential information risks and that remedial actions have been implemented. The DPO will feedback to the Headteacher and to the Governing Board

Appendix 3: Subject Access Requests

Procedures for responding to subject access requests made under 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.

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them.

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

Actioning a subject access request

1. Requests for information must be made in writing; which includes name of individual, address, contact number, email and the reason for the request. This should be addressed to the Data Protection Officer of the school. If the initial request does not clearly identify the information required, then further enquiries will be made.

2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

✓ Passport
✓ Driving licence
✓ Utility bills with the current address
✓ Birth / Marriage certificate
✓ P45/P60
✓ Credit Card or Mortgage statement

This list is not exhaustive.

3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Head teacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The school will not make a charge for the provision of information. However, we may charge for the following:

✓ Should the information request involve multiple copies, the school may charge for photocopying resources, not exceeding the cost of copying and at no more than £10.

5. The response time for subject access requests, once officially received, is 30 days (not working or school days but calendar days, irrespective of school holiday periods).

6. The GDPR allows exemptions as to the provision of some information; therefore all information will be reviewed prior to disclosure.

7. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 30 day statutory timescale.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

9. If there are concerns over the disclosure of information then additional advice should be sought.

10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

12. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

Complaints

Complaints about the above procedures should be made to the Data Protection Officer (DPO) and/or Chair of the Governing Board who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.

Complaints which are not appropriate to be dealt with through the school's complaint procedure or DPO can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.