# DATA PROTECTION POLICY

| | |
|---|---|
| **Name of School** | Church Crookham Junior School |
| **Date of Policy Issue/Review** | Reviewed February 2025 Update May 2026 |

## Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with 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

## 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.

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

| Term | Definition |
|---|---|
| **Personal data** | Any information relating to an identified, or identifiable, individual.<br>This may include the individual's:<br>• Name (including initials)<br>• Identification number<br>• Location data<br>• Online identifier, such as a username<br>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: |

| Term | Definition |
|---|---|
| | • Racial or ethnic origin<br>• Religious or philosophical beliefs<br>• Trade union membership<br>• Health – physical or mental<br>• Sexual orientation or any other protected characteristic |
| **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

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.

## 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.

**Governing Body**

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

**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.

Regular reports of activities are reported 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 Mrs Jo Bickerstaff and is contactable via our School Office or by telephone on 01252-957540.

**Headteacher**

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

**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 or any location that is listed in any subsequent legislation related to data protection
    - 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 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.

| **Collecting Personal Data** | |
|---|---|

Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

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

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.

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

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's Record Retention Schedule.

| **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:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law

- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

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

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

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

Where we transfer personal data to a country or territory outside the European Economic Area (Area or any location that is listed in any subsequent legislation related to data protection), we will do so in accordance with data protection law.

| **Subject Access Requests & other Right of Individuals** | |
|---|---|

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
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

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

- Name of individual

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

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

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents 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.

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.

***If a Subject Access Request (SAR) has been fulfilled and the requester has been informed that the documentation is ready for collection, but it is not collected, the documentation will be securely held at the school for a period of four school weeks. After this time, it will be securely archived in line with the school's data retention procedures.***

**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 previously), 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.

| **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.

| **Photographs and Videos** | |
|---|---|

As part of our school activities, we may take photographs and record images of individuals within our school. We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

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.

| **Data Protection by Design and Default** | |
|---|---|

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

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

| **Data Security and Storage of Records** | |
|---|---|

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.
In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office

- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as two factor authentication.
- 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
- 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)

| **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 put paper-based records in confidential waste 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.

| **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. 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

| **Training** | |
|---|---|

All staff and governors are provided with data protection training as part of their induction process and have an annual refresher update.

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

| **Monitoring Arrangements** | |
|---|---|

The DPO is responsible for monitoring and reviewing this policy.

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

| **Links with other Policies** | |
|---|---|

This data protection policy is linked to our:

- Freedom of information publication scheme
- Child Protection Policy
- Online Safety (Acceptable Use) Policy

## Appendix 1: Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the 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
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:

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

  Records of all breaches will be stored on the school's computer system
- 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 Hampshire IT Services to help in recalling it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Other types of breach that may include:

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

**Data breach guidance for schools**

**Why should we have a breach reporting process?**

The UK GDPR requires that some, but not all data breaches must be reported to the ICO and in some cases the affected individual:

- Reporting to the ICO is required where a breach is likely to result in **a risk** to the rights and freedoms of individuals.

- Reporting a breach to the individual is required where it is likely to result in a **high risk** to their rights and freedoms.

A reportable risk exists when the breach may lead to damage to the individuals whose data have been breached. Examples of damage may include (but are not limited to) discrimination, identity theft or fraud, financial loss and damage to reputation. When the breach involves Special Category Data you should assume such damage is likely.

A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. The school will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again, the risk is higher. In such cases, the school will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them to take steps to protect themselves from the effects of a breach.

If you are not able to demonstrate that you have an appropriate process in place and that your organisation follows it, these timescales may be overlooked and, opportunities to contain the breach may be missed which could lead to enforcement action and/or a fine.

You should therefore have a written breach procedure in place. It should detail the process to follow once a breach has been detected, including how to contain, manage and recover the breach, assess the risk, and notify the breach to the ICO/individual where appropriate. You should make sure that staff are aware of the breach reporting process.

**What is my role as the Data Protection Officer?**

Data Protection Officers play a key role in data breach investigations, notifications on behalf of the school and record keeping. They have a duty to cooperate with the ICO and are a contact point for the ICO and data subjects.
When notifying a breach to the ICO the school must provide the name and contact details of its DPO, or other contact point.

**What should my school do when there is a breach?**

As soon as it becomes aware of a breach, the school must:-

- seek to contain the incident and
- assess the risk that could result from it.

This is important because knowing the likelihood of and the potential severity of the impact on the individual will help the school take effective steps to contain and address the breach. It will also help the school to determine whether it needs to tell the ICO and, if necessary, the individuals concerned.

For example, where personal data is accidentally sent to the wrong person in the school, or to a trusted organisation that the school has a relationship with, the recipient may be asked to either return or securely destroy the data it has received. The school might reasonably expect that the recipient in this example would not read or access the data sent in error and that they would comply with the school's instructions. This would contain the breach, reduce the likelihood of risk to individuals and may make notification to the ICO unnecessary.

**How do we assess the risk?**

Taking into account the specific circumstances of the breach, think about the likelihood of the individual's privacy being impacted by the breach and what that impact might be.

Your assessment should always be objective, taking into account the following criteria:

**The type of breach**
This may affect the level of risk to individuals. For example, a breach where medical information has been disclosed to unauthorised parties has different consequences to a breach where an individual's medical details have been deleted and are no longer available.

**The nature, sensitivity, and volume of personal data**
Usually, the more sensitive the data, the higher the risk of harm will be to the people affected, but you should also consider the context. For example, the disclosure of the name and address of an individual would not generally cause substantial damage but disclosing the name and address of an adoptive parent to a birth parent could have significant consequences for the adoptive parent and child.

**Ease of identification of individuals**
Consider how easy it will be for a person who has access to the personal data to identify specific individuals or match it with other information to identify individuals.

Personal data protected by an appropriate level of encryption will be unintelligible to unauthorised persons without the decryption key. Pseudonymisation can reduce the likelihood of individuals being identified in the event of a breach. This could be as simple as using Child A and Child B instead of names, while keeping a separate record of who it relates to.

**Severity of consequences for individuals**
Depending on the nature and consequences of the personal data involved in a breach (e.g. special categories of data) the potential damage to individuals could be very severe and could lead to identity theft, fraud, physical harm, psychological distress, humiliation or damage to reputation. Breaches of the personal data of children could place them at particular risk of harm.

**Special characteristics of the individual**
A breach may affect personal data of children or other vulnerable individuals, who may be placed at greater risk of danger as a result.

**The number of affected individuals**

Generally, the higher the number of individuals the greater the impact a breach can have. A breach can however have a severe impact on even one individual, depending on the nature and context of the personal data involved.

**General points**
Where the consequences of a breach are more severe, the risk of damage is higher. If in doubt, the school should err on the side of caution and notify the ICO and, where relevant, the individual.

**How should we document the breach?**

Whether you report a breach to the ICO or not, you must keep records of all data breaches.

The records should include:

- What was the breach.
- What caused the breach.
- What personal data was affected including the categories and approx. number of records concerned.
- The categories and approximate number of data subjects concerned.
- What the effects and likely consequences of the breach were.
- What remedial action was taken by the school.

You should also record the reasons for decisions taken in response to a breach, particularly, if a breach is not notified to the ICO.

If a notification to the ICO is delayed the school must be able to provide reasons for the delay and it will help if you have written evidence of this.

If you tell an affected individual about a breach, you should do so in a clear, effective and timely manner and keep a record of the letter/email sent.

**DATA BREACH PROCESS AND FLOWCHART**

**1. School receives a report of a data incident.**

Schools will need to have a procedure in place for reporting data incidents to their Data Protection Officer (DPO). There is a data incident reporting form in this toolkit which your school could use.

Immediate action will need to be taken to contain the incident.

**2. Has a personal data breach occurred?**

The DPO will need to review the information about the incident and establish whether a personal data breach has occurred.

A 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data. This applies regardless of the format in which the personal data is held e.g. electronic, paper, image or recording.

If there are still actions which could be taken to contain the incident these will need to be undertaken immediately.

**3. Assess the risk to individuals.**

If a personal data breach has occurred, the next step is to assess the risk to the individual(s) concerned.

**Is the breach <u>likely</u> to result in a risk to the individual's rights and freedoms?**

If it is **likely** that there will be a risk, then schools must notify the ICO within 72 hours, if it is unlikely then schools do not have to report it.

**Is the breach likely to result in a <u>high risk</u> to the individual's rights and freedoms?**

If it is likely that there will be a **high risk** to the individual's rights and freedoms, then the school must notify the individuals concerned without undue delay.

There could be cases where there will not be a high risk but because the individuals could learn about the breach from a third party (e.g. other parents) it would be best to notify the individual and provide them with your school's account.
NB: Please see our Data Breach Guidance for schools for more details about assessing the risk.

**4. Records**

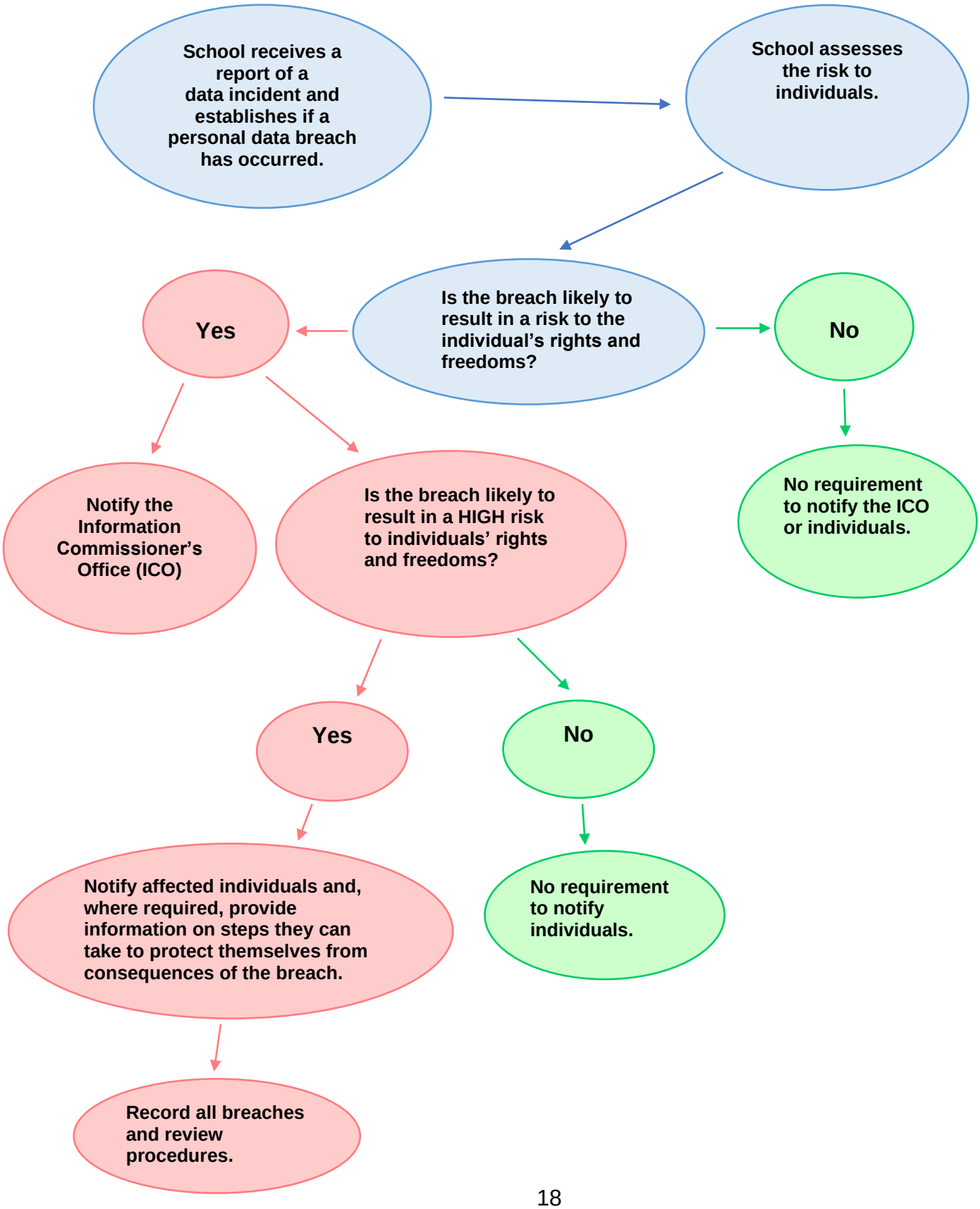
Whether or not the breach was notifiable to the ICO or the individuals a record of the breach should be made, so that you have an audit trail in case of future queries or in case the ICO asks questions about this. There is a data breach recording log in this toolkit which your school could use.

**5. Review**

Following a data breach, a review of your school's procedures should be undertaken to establish whether any changes are required.

If the breach was notifiable to the ICO the school's governing body should be notified of it at the next meeting. All breaches should be included in the Data Protection Officer's Annual Report (our report template can be found at: Annual Report template

**Flowchart showing notification requirements**



**DATA INCIDENT REPORTING FORM**

The aim of this document is to ensure that, in the event of a data incident such as a personal data breach, information can be gathered quickly to document the incident, its impact and actions to be taken to reduce any risk of harm to the individuals affected.

This form can be completed by anyone with knowledge of the incident. It will need to be submitted and reviewed by the Data Protection Officer who will determine the implications for the school, assess whether changes are required to existing school processes and notify the ICO / data subject where appropriate.

| **SUMMARY OF INCIDENT** | |
|---|---|
| Date and time of incident | |
| Nature of breach<br>(e.g. theft/ disclosed in error/ technical problems) | |
| Give a full description of how breach occurred | |
| **PERSONAL DATA** | |
| Give a full description of all the types of personal data involved with the incident.<br>(e.g. name, addresses, health information etc.) | |
| How many individuals /records are affected? | |
| Have the affected individuals been informed of the incident? | |
| Is there any evidence that the personal data involved in this incident has been further disclosed? If so, please provide details | |
| | |

| **IMPACT OF INCIDENT** | |
|---|---|
| What harm is foreseen to the individuals affected?<br><br>(e.g. could the breach increase the risk of identity theft?) | |
| What measures have been taken to minimise the impact of the incident and the likelihood of harm to individuals? | |
| Has the data been retrieved or deleted?<br><br>If yes, state when and how | |
| **REPORTING** | |
| Who first became aware of the incident? | |
| How did they become aware of the incident? | |
| **Form Completed by** | |
| **Position** | |
| **Date** | |

**Data breach recording log**

| Details of breach | | | | | | Measures taken/to be taken | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Date of breach | No of people affected | Nature of breach | Description of breach | Description of personal data | Effects and consequences of breach | Remedial action | Does the ICO need to be notified? If not explain why. | If notifiable, date of notification to ICO | If there was a delay in notifying explain reasons for the delay. | Does the data subject(s) need to be informed? If not explain why. | If data subject(s) need to be informed, date they were informed | Details of notification to any affected organisations | Notes (e.g. result of internal investigation or ICO investigation) |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |

**Other useful information**

**Our data breach case study and answers which can be found in our DPO Training:**

Case study - Data Breach
Case study - Data breach - Answers

**ICO guidance:**

- Personal data breaches guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-UK GDPR/personal-data-breaches/

- Report a breach webpage (which includes personal data breach examples to help assess the severity of a breach and a self-assessment tool to help determine whether the breach needs to be reported to the ICO): https://ico.org.uk/for-organisations/report-a-breach/

- Personal data breach reporting resources which include a webinar: https://ico.org.uk/for-organisations/UK GDPR-resources/pdb/

**DfE Data Protection: A toolkit for Schools** which includes guidance on data breaches and a school data breach case study can be found at: https://www.gov.uk/government/publications/data-protection-toolkit-for-schools

**School Data Breach Court case**:
In ST (A Minor) & Anor v L Primary School (Rev 2) [2020] EWHC 1046 a school was found to have breached the Data Protection Act by sending a letter about the behaviour of a child with Down's Syndrome to a group of parents without the child's parent's consent.

**ICO Action taken**
In May 2023, the ICO issued a public reprimand to Parkside Community Primary School for failure to adequately protect personal data which resulted in personal data including special category data about specific children being disclosed in a classroom environment to other children. (The full details of circumstances are not provided in the reprimand document, but refresher training in the use of electronic whiteboards is mentioned). The reprimand also records a breach of process in failing to report the data breach within the school.

https://ico.org.uk/media/action-weve-taken/reprimands/4025365/parkside-community-primary-school-reprimand-20230523.pdf

**Cyber security in schools: questions for governors and trustees (July 2020):**
https://www.ncsc.gov.uk/information/school-governor-questions