A picture containing text, vector graphics

Description automatically generatedWINGATE COMMUNITY NURSERY SCHOOL

DATA PROTECTION POLICY

|  |  |  |
| --- | --- | --- |
| **Approved by:** | Becky Wood | **Date:** September 2023 |
| **Last reviewed on:** | September 2022 | |
| **Next review due by:** | September 2024 | |

# 1. Aims

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

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

# 2. Legislation and guidance

This policy meets the requirements of the:

* UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by [The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020](https://www.legislation.gov.uk/uksi/2020/1586/made)
* [Data Protection Act 2018 (DPA 2018)](http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted)

It is based on guidance published by the Information Commissioner’s Office (ICO) on the [UK GDPR](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/) and guidance from the Department for Education (DfE) on [Generative artificial intelligence in education](https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education).

It also reflects the ICO’s [code of practice](https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf) 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](http://www.legislation.gov.uk/uksi/2005/1437/regulation/5/made), which gives parents the right of access to their child’s educational record.

# 3. Definitions

| term | definition |
| --- | --- |
| **Personal data** | Any information relating to an identified, or identifiable, living individual.  This may include the individual’s:   * Name (including initials) * Identification number * Location data * Online identifier, such as a username   It may also include factors specific to the individual’s physical, physiological, genetic, mental, economic, cultural or social identity. |
| **Special categories of personal data** | Personal data which is more sensitive and so needs more protection, including information about an individual’s:   * Racial or ethnic origin * Political opinions * Religious or philosophical beliefs * Trade union membership * Genetics * Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes * Health – physical or mental * Sex life or sexual orientation |
| **Processing** | Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.  Processing can be automated or manual. |
| **Data subject** | The identified or identifiable individual whose personal data is held or processed. |
| **Data controller** | A person or organisation that determines the purposes and the means of processing of personal data. |
| **Data processor** | A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller. |
| **Personal data breach** | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. |

# 4. The data controller

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

The school is registered with the ICO and has paid its data protection fee to the ICO, as legally required.

# 5. Roles and responsibilities

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

5.1 Governing board

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

5.2 Data protection officer

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. These include the Acceptable Use Policy, Record Keeping and Retention Policy, Photographic and Video Policy and Freedom of Information statements.

They will produce an annual audit of the schools GDPR compliance which they will report directly to the governing body along with 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 Darren Hobson and is contactable via email [info@mobile-sbm.com](mailto:info@mobile-sbm.com) or by telephone on 07368508685.

5.3 Headteacher

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

5.4 All staff

Staff are responsible for:

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

# 6. Data protection principles

The UK GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

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

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

# 7. Collecting personal data

7.1 Lawfulness, fairness and transparency

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

* The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
* The data needs to be processed so that the school can **comply with a legal obligation**
* The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone’s life
* The data needs to be processed so that the school, as a public authority, can **perform a task** **in the public interest or exercise its official authority**
* The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual’s rights and freedoms are not overridden
* The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

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

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

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

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

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

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

7.2 Limitation, minimisation and accuracy

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

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

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

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

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school’s record retention schedule.

# 8. Sharing personal data

We will not normally share personal data with anyone else without consent, 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

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

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

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

# 9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a ‘subject access request’ to gain access to personal information that the school holds about them. This includes:

* Confirmation that their personal data is being processed
* Access to a copy of the data
* The purposes of the data processing
* The categories of personal data concerned
* Who the data has been, or will be, shared with
* How long the data will be stored for, or if this isn’t possible, the criteria used to determine this period
* Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
* The right to lodge a complaint with the ICO or another supervisory authority
* The source of the data, if not the individual
* Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
* The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

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

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

**Our procedure for handling of subject access requests is set out in Appendix 1.**

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.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil’s ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

* May ask the individual to provide 2 forms of identification
* May contact the individual via phone to confirm the request was made
* Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
* Will provide the information free of charge
* May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

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

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

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

9.4 Other data protection rights of the individual

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

* Withdraw their consent to processing at any time
* 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 DPO. If staff receive such a request, they must immediately forward it to the DPO.

# 10. Parental requests to see the educational record

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

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

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

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

# 11. CCTV

We may use CCTV in various locations around the school site to ensure it remains safe. We will follow the [ICO’s guidance](https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance/) for the use of CCTV, and comply with data protection principles.

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.

See our CCTV policy for further information.

# 12. Photographs and videos

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

We will obtain written consent from for photographs and videos to be taken of our pupils for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used and will set this information out in photograph consent forms. There may be a need to obtain one off consent during the year for specific events not covered by our photo consent form.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this. It may be necessary for us to prevent any photography by parents if we feel this is necessary to safeguard our pupils at particular events or in certain circumstances. See our Photographic and Video Policy for further information.

Where the school takes photographs and videos, uses may include:

* Within school on notice boards and in school 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 Photographic and Video Policy for more information on our use of photographs and videos.

# 13. Use of Artificial Intelligence

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

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

If personal and/or sensitive data is entered into an unauthorised generative AI tool, school will treat this as a data breach, and will follow the personal data breach procedure.

# 14. Data protection by design and default

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

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

# 15. Data security and storage of records

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

In particular:

* Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
* Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
* Where personal information needs to be taken off site, staff must sign it in and out from the school office
* Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
* Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
* Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our E-Safety and Acceptable Use Policies)
* Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

# 16. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school’s behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

# 17. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:

* A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
* Safeguarding information being made available to an unauthorised person
* The theft of a school laptop containing non-encrypted personal data about pupils

# 18. 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.

# 19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

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

# 20. Links with other policies

This data protection policy is linked to our:

* Freedom of information publication scheme
* Photographic and Video Policy
* Acceptable Use Policy
* Data Breach Procedure
* Record Keeping and Retention Policy
* Child Protection and Safeguarding Policy
* E-Safety Policy

### Appendix 1: Subject Access Request Procedure

Individuals can submit a subject access request (SAR) to the school in any form. There are designated forms that can be filled in for such requests and these are available in school. However, requests can also be made verbally or in writing in other formats, for example via email.

The school may need to undertake checks where necessary on the identity of the individual making the request before releasing the information if this is not clear.

The process to be followed in the event of a member of staff receiving a SAR is as follows;

Member of staff receives SAR

Full details are passed to the Head teacher on the same working day

*(or within 24 hours where this is not possible)*

*Head teacher informs the DPO on the same working day*

*(or within 24 hours where this is not possible)*

*The Head teacher & Chair of Governors gather the information requested in conjunction with the DPO*

*The information is provided to the individual within 1 month*

A picture containing text, vector graphics

Description automatically generatedWINGATE COMMUNITY NURSERY SCHOOL

DATA BREACH PROCEDURE

SEPTEMBER 2023

|  |  |  |
| --- | --- | --- |
| **Approved by:** | Becky Wood | **Date:** September 2023 |
| **Last reviewed on:** | 14 September 2023 | |
| **Next review due by:** | September 2024 | |

**Policy Statement**

1. Schools are responsible for large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the unlikely event of data being lost or shared inappropriately, it is imperative that the appropriate action is taken to minimise any associated risk as soon as possible.

# Purpose

1. This policy sets out the procedure to be followed by school staff and governors when a potential data protection breach takes place. It sets out the decision process by which a potential breach is logged, investigated and a breach determined. The final stages are to decide whether notification of a breach to either the data subjects or the ICO is necessary.

# Scope

1. This procedure applies to all personal and sensitive personal data held by the school.

# Definitions

|  |  |
| --- | --- |
| **Data** | A collection of facts from which conclusions may be drawn. |
| **Personal data *(as defined by the Data Protection Act 1998)*** | Data that relates to a living individual who can be identified from that data, or from that data and other information that comes into the possession of the Data Controller. For example:   * Name * Address and postcode * Date of birth |
| **Special Category Data *(Formerly Sensitive Data)*** | Personal data consisting of:   * Racial or ethnic origin * Political opinions * Religious or similar beliefs * Trade union membership * Physical or mental health or condition * Sexual life * Genetic or Biometric Data |
| **Data Controller** | A person or organisation that determines the purposes for which, and the manner in which, personal information is to be processed. The school should be registered as a Data Controller. |
| **DPA** | Data Protection Act 1998 |
| **Data Processor** | A person who processes personal information  on a data controller's behalf. Anyone responsible for the disposal of confidential waste is also included under this definition. A school employee is not a data processor. |
| **Data Subject** | The living individual who is the subject of the data/personal information. |
| **UK GDPR** | UK General Data Protection Regulation (new European legislation that will supersede the DPA) |
| **LADO** | Local Authority Designated Officer |
| **Potential Data Breach** | The potential loss, theft, corruption,  inappropriate access or sharing of personal, or sensitive personal data. |
| **Phishing / blagging** | The act of tricking someone into giving out confidential information. |
| **DCC** | Durham County Council. |
| **ICO** | Information Commissioner’s Office  The ICO is the UK's independent public body set up to promote access to official information and protect personal information by promoting good practice, ruling on eligible complaints, providing information to individuals and organisations, and taking appropriate action when the law is broken. |
| **Ransomware** | Illegal software that encrypts users’ data, then holds the school to ransom demanding payment of hundreds of pounds to provide the password. |
| **Schedule 2 conditions**  **(as amended by the UK GDPR) that may be relevant:** | (i) consent  (ii) needed for contractual performance  (iii) needed to comply with legal obligations  (iv) needed to protect vital interests  (v) needed to perform a task in the public interest or in the exercise of official authority |
| **Schedule 3 conditions**  **(as amended by the UK GDPR) that may be relevant:** | 1. explicit consent 2. necessary processing by an employer 3. to protect vital interests 4. where the data has been manifestly made public by the subject 5. necessary for judicial proceedings 6. necessary for substantial public interest reasons 7. necessary health processing 8. necessary for archiving purposes |
| **Actionfraud** | <http://www.actionfraud.police.uk/> National cybercrime reporting centre. |

# Legal Context

1. The Data Protection Act regulates the processing (use) of information relating to living individuals, including the obtaining, holding, use or disclosure of such information.

1. Principle 7 of the Data Protection Act 1998 states that organisations which process personal data must take “appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data”.

**What is a potential data breach?**

1. A potential data breach occurs, in general, when the Data Protection Act is not complied with in the processing of personal information. What this means is that the failure to comply with any of the 8 data protection principles can be considered a breach. The 8 data protection principles are as follows:

* + Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless

* + 1. at least one of the conditions in Schedule 2 is met, and

* + 1. in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met and the processing is proportionate to the aim pursued and respects the essence of data protection rights.
  + Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

* + Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

* + Personal data shall be accurate and, where necessary, kept up to date.

* + Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

* + Personal data shall be processed in accordance with the rights of data subjects under this Act.

* + Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

* + Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

1. This Data Breach Procedure aims to ensure that the school fulfils the seven Data Protection Principle and takes appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

1. A potential data security breach can happen for a number of reasons:

* + Loss or theft of data or equipment on which data is stored
  + Accidentally sharing data with someone who does not have a right to know this information
  + Inappropriate access controls allowing unauthorised use
  + Equipment failure
  + Human error resulting in data being shared with someone who does not have a right to know
  + Hacking attack
  + ‘Blagging’ offences where information is obtained by deceiving the school to disclose personal information.

Examples of these include:

* The loss or theft of all or part of a service user’s personal information, containing identifying information and/or details of their current personal circumstances.

* + Sharing of personal and/or sensitive service user information when consent has not been given and there is no legal basis to override this. Or more information is sent than is required. For example, if you send a whole medical file when a sickness absence form is all that is needed.

* + Emailing service user personal and/or sensitive personal information outside the school without appropriate security encryption measures in place. For example, if you send a case review notes record over an unsecured email system.

1. The list is indicative but not exhaustive. If you are, in any way, unsure whether or not a potential breach has taken place the schools Data Protection Officer should be contacted and legal advice may be sought.

**What about an Information Communication Technology (ICT) breach?**

1. If a potential breach involves an ICT device or service, such as a lost laptop, an errant email or a stolen USB stick, then technical advice should be sought from the ICT service provider.

## Mandatory Procedures

1. When a potential breach has occurred, the school will need to investigate it to determine if an actual breach has occurred. In that process, there are four steps to manage and investigate a potential breach. They are:

* + Reporting
  + Containment and Recovery
  + Investigating/Managing
  + Evaluation and response

1. For each stage, there is **a key decision.** The following steps set out the decision process at each stage. (See also the flowchart at end of document.)

1. The report template is included (at the end of the document) to help staff identify and manage potential breaches.

# Reporting the Potential Data Breach Responsible Officer

**Data protection officer**

1. **The first decision stage** is to determine whether a potential breach has occurred. If you discover an incident that meets the criteria set out earlier (i.e. breaches any of the criteria set out at paragraph 6 above), you need to start this process.

1. Keep a log of all potential and investigated breaches. The log can then be analysed to ensure that any lessons learnt from breaches can be implemented.
2. Record the following in the log if known:

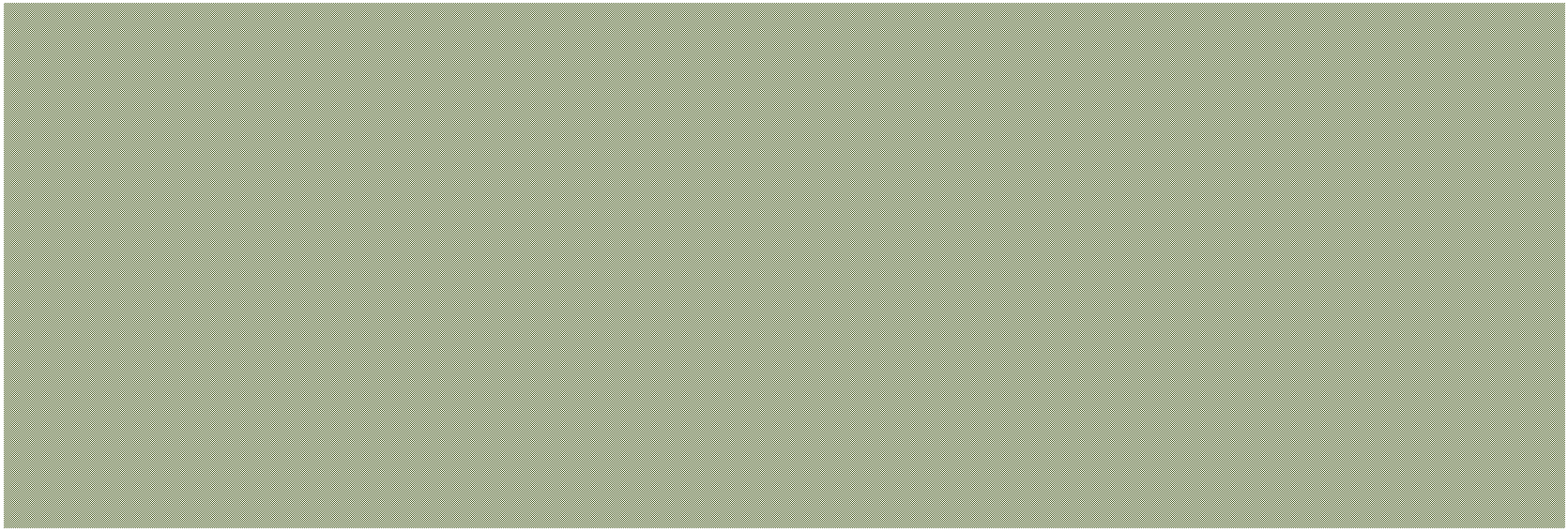
* 1. Date of incident
  2. Date you were made aware of the potential breach
  3. Location of incident
  4. Nature of incident, that is, is it a loss, theft, disposal, unauthorised disclosure?
  5. Nature of data involved, list all data elements. For example, whether it is names, files, dates of birth, or reference numbers
  6. What security protection was on the data? Is it protected by a password, encryption, or something else?
  7. Is there a back up of the data, if so where?
  8. Number of people potentially affected, an estimate should be provided if no precise figure can be given.
  9. Details of any steps taken to retrieve data or to contain the breach if it involved unauthorised access or potentially compromised security.

**Note:** If the incident involves the theft, for example, of a bag containing personal documents or a laptop, the theft must be reported to the Police.

# Containment and Recovery Responsible Officer

**Data protection officer**

1. The **second decision stage** is to consider whether the potential breach needs an investigation template or whether it can be contained within the school or DCC services. The focus is on whether the potential breach has been contained. If so, this will be logged as a **near miss** and no further action will be taken.
2. The reasons behind the near miss will be analysed and any trends or learning outcomes will be shared across the services to prevent future breaches.



**Worked example.**

A teacher contacts the head to say that an envelope containing sensitive personal information about the medical condition of a pupil was given to the wrong Educational Psychologist. The envelope has not been opened and the school has been contacted by the Educational Psychology Service. The school will need to collect the envelope to secure the information. In this instance the information was contained. This would be recorded as a ‘near miss’.

1. If the breach has not been contained then the school should follow the data breach investigation template. A copy of this template at the end of this document.
2. The Data Protection Officer will want to take steps to contain the potential breach. They will want to recover the information and they will need to inform their Chair of governors.
3. **If a pupil is potentially in danger from the breach, their safety is a priority and they must be protected. Follow safeguarding procedures. Once they are safe, then an investigation can commence.**

**What are the criteria for deciding whether a potential breach requires an investigation?**

1. The decision to investigate formally will depend mainly on whether the information has been disclosed and is uncontained. Both of these will also indicate the possible effect it will have on the people whose data has been disclosed. The following are some of the criteria that indicate when a potential breach needs further investigation and cannot be considered contained by the service:

* + Sensitive personal information is disclosed to anyone who does not work for the school or LA and does not have a need to know.
  + Sensitive personal information of pupils or staff is lost or stolen.
  + Sensitive personal information, such as case review documentation, is emailed to several people who do work for the LA but who do not have a need to know.

# Investigating the Potential Data Responsible Officer

## Breach Data protection officer /

## Headteacher /

## Chair of governors

1. When a potential breach meets the criteria for further investigation, the school needs to investigate the loss and produce a short report. In general, the report needs to answer four interrelated questions.

* + What caused or allowed the breach to occur?
  + Do the people affected by the breach need to be informed?
  + Does the ICO need to be notified?
  + What are the lessons to be learned to avoid a similar breach in the future?



**Worked example**

The school secretary reports that a child’s assessment from the Educational Psychologist went to the wrong address. The person at the wrong address opened the assessment and read it. They contacted the school. This is a potential breach that needs to be investigated. It cannot be contained because the letter has been opened. If the letter had been collected before it had been opened, then it could be considered to have been contained. This needs further investigation, and may need to be referred to the ICO. The safety of the child should also be considered and additional safeguarding procedures may need to be followed.

1. A template for investigating data breaches is attached at the end of the document.

1. Beyond the containment and recovery phase, the investigation may reveal that the people affected by the breach need to be informed. When the school decides to notify the affected persons, it should have a clear purpose, for example, to enable individuals who may have been affected to take steps to protect themselves. If there is a safeguarding concern identified, the school should immediately follow its safeguarding procedures, for example, if the identity of a looked after child (LAC) at risk has been disclosed, this could affect the safety of the child and measures will need to be taken to protect the safety of the family. In extreme cases, for instance if a member of staff has lost or published personal data affecting children, it may be necessary to instigate disciplinary measures against the member of staff and consider referral to the LADO for further advice.
2. Please note: This decision is to tell the data subject so that they can take any steps they feel necessary to protect their personal information, such as from identity theft. This is not the formal notification of the ICO which is covered in the fourth decision stage following a formal data breach.
3. At the end of the investigation, the school may want to contact the data subject(s) and explain what went wrong and what has been done to fix it. A copy of the full data breach investigation report is not normally sent.

1. The investigation report will suggest whether the incident needs to be logged as a formal data breach.

# Managing the Potential Breach Responsible Officer

**Data protection officer**

1. Once a potential data breach report is completed the **third decision point** is reached. The decision now is whether the potential breach is to be logged as a formal data breach. **What are the criteria for recommending a formal data breach?**
2. The primary consideration will be the wellbeing of the people affected by the breach.

1. The following questions will help with making that decision.

* + What type of data is involved?
  + How sensitive is it? Is it sensitive because of its very personal nature (health records) or because of what might happen if it is misused (bank account details)?
  + What has happened to the data? If data has been stolen, could it be used to harm the individuals it relates to?
  + What does the data tell a third party about the individual? Is it only one detail about them, such as a telephone number, or does it include other details that could help a fraudster build a detailed picture?
  + How many people are affected?
  + Who are the people affected? For example, are they staff, customers, clients, suppliers, or vulnerable children and adults?
  + What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?

1. The severity of any potential breach needs to be considered in terms of the sensitivity of the information and the number of people involved. The matrix [Table 1] shows when a potential breach becomes an actual breach requiring further formal assessment. *The table is for guidance only and other circumstances may have to be considered.*
2. The school should use Table 1, below, when considering whether to recommend if a potential data breach investigation should result in the recording of a formal data breach.

**Table 1**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Number  of  People involved | 1000+ |  |  | |  |  | |  |
| 100 |  |  | |  |  | |  |
| 50 |  |  | |  |  | |  |
| 5 |  |  | |  |  | |  |
| 1 |  |  | |  |  | |  |
|  | e.g.  Name, address | e.g.  National Insurance number | | e.g. Bank details, medical information | e.g. Details of a vulnerable child. | | e.g Full medical  files or criminal  file |
|  | Sensitivity of the Information | | | | | | | |
| Key | **Unlikely to require recommending as a formal breach** | | | **Consideration should be given to recommending as a formal breach** | | | **Likely to require recommending as a formal breach** | |

1. The table is only a guide. **The risk of harm to the individuals involved should be considered as the determining factor.**

**Worked example**

Here is a worked example to understand the difference between a near miss, a potential breach and a formal data breach. The formal data breach requires recording on the formal data breach log. All breaches start as potential breaches and then are recorded as near miss, potential breach, or formal breach.



**Near Miss**

Some data security breaches will not lead to risks beyond inconvenience to those who need the data to do their job. For example, a damaged laptop where the files are backed up and can be recovered, has a lower level of risk and can be recovered and managed by the school. This has to be investigated as potential breach. As the information can be recovered or reconstructed and the information is not in the public domain, then the data subjects would not have suffered damage or distress. It would be logged as a **near miss.** An apology would not need to be sent.

**Potential data breach**

If the data cannot be recovered and it will have an effect on the data subject because the school has to reconstruct the data set. Even though the data is not in the public domain, it would be investigated and logged as a potential breach. The investigation should reveal why the data was stored in such a way it could become corrupted and was not recoverable. If the data subject was not affected directly by the breach, then they would not need to be informed. If they were affected, such as a missed appointment as a result, then they would need an apology.

**Formal data breach**

A spreadsheet with the medical assessments including psychological assessments of vulnerable children was emailed to 400 taxi firms. The breach cannot be contained. It involves sensitive information of more than 5 people. This would require an investigation.

The investigation should recommend it be logged as a formal data breach based on the amount of information, that it was in the public domain, the sensitivity of the information and the potential harm to the children. The harm to the individuals would be greater because their information was in the public domain. An apology would need to be issued. This would need to be logged as a formal breach and the school would need to consider whether it will inform the ICO.

# Final Evaluation and Response Responsible Officer

# Headteacher /

# Data protection officer /

# Chair of governors

1. The final evaluation process is done by the Head, DPO and Governing Body to consider the causes of the breach and the lessons that need to be learned. The investigation report indicates how effective the school was in response to the breach. The school should also seek advice from the School and Governor Support Service.
2. The school should implement any actions highlighted by the report**.**

# Formal Notification of Breaches Responsible Officer

**Data Protection Officer/**

**Heateacher/**

**Chair of governors**

1. The **fourth decision stage** is whether the data breach was severe enough to require the school to inform the Information Commissioner’s Office. The decision to notify the ICO will be made by the school with additional advice from the School and Governor Support Service.

**Please note** that this decision stage is different from notifying a data subject of the data breach.

Breach Template

Has there been a data breach?

Complete Investigation log (Para 14)

No

Notify Subjects

No further action

Yes

This is a “Near Miss” - review systems to reduce the possibility of a future data breach

Has the breach been contained?   
(Para 17)

Yes

Notify ICO

Does this meet data subject notification criteria?

(Para 25-26)

No

Is this a “Formal breach”?

(Para 29-34)

Yes

Is this a “Serious Breach”?

(Para 37)

Yes

No

No

No

Yes

No further action – but review systems to reduce the possibility of a future data breach

No further action – but review systems to reduce the possibility of a future data breach

Follow data breach template and complete investigation

Follow safeguarding procedures if any risk to data subjects

(Para 21)

# Data Breach Investigation Report Template

**Root Cause Analysis (RCA) - Investigation Report Template – Guidance.**

## Write your investigation report in the right hand column (column B)

To help in writing the report, refer to summary guidance in column A.

Additional help can be found in the ‘Guide to RCA investigation report writing’.

If, when you are carrying out your investigation, there is no information against a heading, please explain why this is the case. (For example, if you do not know the date of an incident, but only the date it was reported, then leave the incident date blank and explain the date is not known.)

If issues arise which require a new heading this can be added as a new row.

## Once you have completed column B, you need to delete column A. \* All that is required is column B\*

First, delete all guidance both here and in the template below.

A copy of this report will need to be retained in the school and may be needed by other agencies (Police, ICO, Legal Team) in assisting the school in dealing with the consequences of the breach.

|  |  |
| --- | --- |
| **Column A** | **Column B** |
| **Quick reference guide** | **Type your investigation report in this column** |
| **Incident Date** |  |
| **Incident Number** | Add your number |
| **Author(s) / Investigating Officer** | Name of person |
| **Report Date** | Date |
| **Incident description and**  **consequences**  (Concise incident description,  including number of data subjects.) | The personal information of 25 vulnerable children were disclosed when an email was sent to external transport list rather than an internal transport list. |
| **Information Recovered** | Yes or No. |
| **Decision as to whether those individuals whose data has been breached and are to be notified.** | *Example only (please delete and add your own findings)*  The 25 people included bank details. The individuals concerned have been notified to allow them to be vigilant for any suspicious activity on their account. |
| **Chronology of events**  (For complex cases any summary  timeline included in the report should be a summary.) | The key points of the event: when discovered, when last use of data, when authority notified, when information recovered if recovered, when data subject informed of risk etc. |
| **Contributory factors**  (A list of significant contributory facts.) | Over the years email addresses had been added, causing the team to lose track of the internal and external lists. |
| **Root Causes**  (These are the most fundamental underlying factors contributing to the incident that can be addressed. Root causes should be meaningful (not sound bites such as communication  failure) and there be a clear link, by analysis, between root CAUSE and EFFECT.) | Staff involved have not had training on use of internal and external lists. Internal and external lists have names that are only different by one letter. There is no procedure for creating distributions lists to be used by service. |

|  |  |
| --- | --- |
| **Lessons learned**  (Key issues identified which may not have contributed to this incident but from which others can learn.) | The external lists should be marked clearly and consistently as external. |
| **Type of breach** | Please tick one of the following:  Near miss  Potential breach  Further action:  *please provide details* |
| No further actions  Formal breach |
| **Recommendations**  (Numbered and referenced)  Recommendations should be directly linked to root causes and lessons learned. They should be clear but not detailed. (Detail belongs in the action plan.) It is generally agreed that key recommendations should be kept to a minimum whereever possible. All recommendations are to be Specific, Measurable, Achievable, Realistic and Timely. – SMART. | Ensure all email lists are reviewed so that external lists are clearly marked. All staff are instructed about the use of external email lists. |
| **Arrangements for shared learning** (Describe how learning has been or will be shared with staff and other organisations.) | *Example only (please delete and add your own findings)*   * Share findings with other schools sharing similar activities. * Share findings to identify opportunities for sharing outside the organisation. |
| **Outcome**  (The conclusion of the investigation should state whether the author believes the breach should be logged formally or not.) | *Example only (please delete and add your own findings)*  As the breach resulted in sensitive personal information being inappropriately shared with more than 10 people, it is recommended that this be recorded as a formal data breach. |
| **Headteacher, Data Protection Officer and Chair of governors**  **Date** |  |