UPDATED MARCH 2021

REVIEW MARCH 2022

ST. JOSEPH'S CATHOLIC PRIMARY SCHOOL

DATA PROTECTION POLICY

1. Aims & Objectives:

The aim of this policy is to provide a framework to enable staff, parents and pupils to understand:

- The law regarding personal data
- How personal data should be processed, stored, archived and deleted/destroyed
- How staff, parents and pupils can access personal data

1.1. It is a statutory requirement for all schools to have a Data Protection Policy:

http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/a00201669/statutory-policies-for-schools

1.2. Data Protection Principles

The Data Protection Act 1998 establishes eight principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully;

2. Personal data shall be obtained only for one or more specified and lawful purposes;

3. Personal data shall be adequate, relevant and not excessive;

4. Personal data shall be accurate and where necessary, kept up to date;

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

6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;

7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;

8. 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 data protection.

2. Data Types

Not all data needs to be protected to the same standards, the more sensitive or potentially Damaging the data is, the better it needs to be secured. There is inevitably a compromise between usability of systems and working with data. In a school environment staff are used to managing risk, for instance during a PE or swimming lesson where risks are assessed, controlled and managed. A similar process should take place with managing school data.

The DPA defines different types of data and prescribes how it should be treated.

The loss or theft of any Personal Data is a *"Potential Data Breach"* which could result in legal action against the school. The loss of sensitive personal data is considered much more seriously and the sanctions may well be more punitive.

2.1. Personal data

The school will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:-

- Personal information about members of the school community – including pupils / students, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, disciplinary records.
- Curricular / academic data e.g. class lists, pupil / student progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records, disciplinary records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

2.2. Sensitive Personal data

Sensitive personal data is defined by the Act as information that relates to the following 8 categories: race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexual life and criminal offences, criminal proceedings. It requires a greater degree of protection and in a school would include:-

- Staff Trade Union details
- Information on the racial or ethnic origin of a child or member of staff
- Information about the sexuality of a child, his or her family or a member of staff
- Medical information about a child or member of staff
- Information relating to any criminal offence of a child, family member or member of staff.

Note – On some occasions it is important that medical information should be shared more widely to protect a child - for instance if a child had a nut allergy how it should be treated. Where appropriate written permission should be sought from the parents / carers before posting information more widely, for instance in the staff room.

2.3. Other types of Data not covered by the act.

This is data that does not identify a living individual and therefore is not covered by the remit of the DPA this may fall under other access to information procedures. This would include Lesson Plans (where no individual pupil is named), Teaching Resources, and other information about the school which does not relate to an individual. Some of this data would be available

publically (for instance the diary for the forthcoming year), and some of this may need to be protected by the school (If the school has written a detailed scheme of work that it wishes to sell to other schools). Schools may choose to protect some data in this category but there is no legal requirement to do so.

The ICO provide additional information on their website See http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions

3. Responsibilities

The Headteacher and Governing Body are responsible for Data Protection, they may appoint a SIRO
to manage data.

3.1. Risk Management - Roles

The school's Senior Information Risk Officer **(SIRO)** is Mrs R Williams. This individual will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners **(IAOs**)

The school will identify Information Asset Owners (IAOs) for the various types of data being held
(E.g. pupil / student information / staff information / assessment data etc.). The IAOs will manage
and address risks to the information and will understand:

- what information is held, for how long and for what purpose, • how information has been amended or added to over time, and
- who has access to protected data and why.

3.2. Risk management - Staff and Governors Responsibilities

- Everyone in the school has the responsibility of handling personal information in a safe and secure manner.
- Governors are required to comply fully with this policy in the event that they have access with personal data, when engaged in their role as a Governor.

4. Legal Requirements

4.1. Registration

The school must be registered as a Data Controller on the Data Protection Register held by the Information Commissioner and each school is responsible for their own registration): http://ico.org.uk/for_organisations/data_protection/registration

4.2. Information for Data Subjects (Parents, Staff)

In order to comply with the fair processing requirements of the DPA, the school will inform parents / carers of all pupils / students and staff of the data they collect, process and hold on the pupils / students, the purposes for which the data is held and the third parties (e.g.

LA, DfE, etc.) to whom it may be passed. This privacy notice will be passed to parents / carers through a letter. More information about the suggested wording of privacy notices can be found on the DfE website:

http://www.education.gov.uk/researchandstatistics/datatdatam/a0064374/pn

See Appendix 2

5. Transporting, Storing and Deleting personal Data

 The policy and processes of the school will comply with the guidance issued by the ICO here https://ico.org.uk/media/action-weve-taken/self-assessments/2790/report-dp-guidance-forschools.pdf

5.1. Information security - Storage and Access to Data

5.1.1. Technical Requirements

- The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.
- Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.
- All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.
- Personal data can only be stored on school equipment (this includes computers and portable storage media (where allowed). Private equipment (ie owned by the users) must not be used for the storage of personal data.
- St. Joseph's RC Primary has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups. (the school will need to set its own policy, relevant to its physical layout, type of ICT systems etc.)

5.1.2. Portable Devices

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected,
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected),
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

5.1.3. Passwords

- All users will use strong passwords which must be changed regularly. User passwords must never be shared. It is advisable NOT to record complete passwords, but prompts could be recorded.

5.1.4. Images

- Images of pupils will only be processed and transported by use of secure posting via the School Photographer or where permission has been obtained in the privacy agreement.
- Images will be protected and stored in a secure area.

5.1.5. Cloud Based Storage

- St Joseph's R C Primary School has clear policy and procedures for the use of "Cloud Based Storage Systems" and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.
  http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx

5.2. Third Party data transfers

- As a Data Controller, the school / academy is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.
  http://ico.org.uk/for_organisations/data_protection/topic_guides/data_sharing

5.3. Retention of Data

- The guidance given by the Information and Records Management Society – Schools records management toolkit will be used to determine how long data is retained.
- Personal data that is no longer required will be destroyed and this process will be recorded.

5.4. Systems to protect data

5.4.1. Paper Based Systems

- All paper based OFFICIAL or OFFICIAL – SENSITIVE (or higher) material must be held in lockable storage, whether on or off site.
- Paper based personal information sent to parents will be checked by office staff members, before the envelope is sealed.

5.4.2. School Websites

- Uploads to the school website will be checked prior to publication ensure that personal data will not be accidently disclosed and that images uploaded only show pupils where prior permission has been obtained.

5.4.3. E-mail

E-mail cannot be regarded on its own as a secure means of transferring personal data.

- Sensitive information will only be transferred by secure email addresses; these have been issued to all staff members. There is also the school's secure email address which is only accessible to senior office staff: admin.stjosephs@school.hartlepool.gov.uk Data Breach – Procedures

On occasion, personal data may be lost, stolen or compromised. The data breach includes both electronic media and paper records, and it can also mean inappropriate access to information.

- In the event of a data breach the SIRO will inform the head teacher and chair of governors
- The school will follow the procedures set out in Appendix 7

Appendix 1 Links to resources and guidance ICO

Guidance for schools

http://ico.org.uk/for_organisations/sector_guides/~/media/documents/library/Data_Protection/Research_and_reports/report_dp_guidance_for_schools.ashx

A downloadable guide for schools

Specific information for schools is available here http://ico.org.uk/for_organisations/sector_guides/education Specific information about

use of Cloud Based technology

http://ico.org.uk/for_organisations/data_protection/topic_guides/online/cloud_computing

Specific Information about CCTV

http://ico.org.uk/for_organisations/data_protection/topic_guides/cctv

Information and Records Management Society – Schools records management toolkit

http://www.irms.org.uk/resources/information-guides/199-rm-toolkit-for-school A

downloadable schedule for all records management in schools

Disclosure and Barring Service (DBS) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/143669/handling-dbs-cert.pdf Details of storage and access to DBS certificate information.

DFE Privacy Notices https://www.gov.uk/government/publications/data-protection-and-

privacy-privacy-notices

DFE Use of Biometric Data

https://www.gov.uk/government/publications/protection-of-biometric-information-ofchildren-in-schools

Appendix 2 Privacy Notices (May 2016)

Links to LA Information; Privacy and data protection when sending :

Processing images off site (staff to prepare learning journeys away from the school building)

On occasion the school permits data to be processed off site by members of staff (e.g. preparing learning journeys).

Text Service

St Joseph's R C Primary School uses a texting service managed by Teachers2Parents to communicate with parents. Please contact Mrs Allan in the school office for further information or if you want to opt out of this arrangement.

Class Lists

St Joseph's R C Primary School share class lists (first names only) with parents, for instance in helping children to write birthday and Christmas cards. Please contact Mrs Allan for further information or if you want to opt out of this arrangement.

Appendix 3 Glossary

Data Protection Act 1998: All personal data which is held must be processed and retained in accordance with the eight principles of the Act and with the rights of the individual. Personal data must not be kept longer than is necessary (this may be affected by the requirements of other Acts in relation to financial data or personal data disclosed to Government departments). Retention of personal data must take account of the Act, and personal data must be disposed of as confidential waste. Covers both personal data relating to employees and to members of the public.

ICO The Information Commissioner's office. This is a government body that regulates the Data Protection Act.

The ICO website is here http://ico.org.uk/

Data Protection Act 1998: Compliance Advice. Subject access – Right of access to education records in England: General information note from the Information Commissioner on access to education records. Includes timescale (15 days) and photocopy costs.

Data Protection Act 1998: Compliance Advice. Disclosure of examination results by schools to the media: General information note from the Information Commissioner on publication of examination results.
Education Act 1996: Section 509 covers retention of home to school transport appeal papers. (By LA)

Education (Pupil Information) (England) Regulations 2005: Retention of Pupil records

Health and Safety at Work Act 1974 & Health and Safety at Work Act 1972: Retention requirements for a range of health and safety documentation including accident books, H&S manuals etc.

School Standards and Framework Act 1998: Retention of school admission and exclusion appeal papers and other pupil records.

Appendix 4 Impact Levels and Marking

Schools may wish to proactively mark data in order to protect it more carefully.

The Government now uses 5 levels of proactive marking. Unless otherwise specified data falls into the "Official" category. All data in schools will be Public, Official or Official Sensitive.

Type of Data	**Marking**
Public This would include any information not containing any personal data, or information in the public domain. This includes :- • *Lesson Plans and Teaching resources* • *Public Documents such as policies etc.*	***Schools could mark this as either "Public Domain" or " Not Protectively marked"***
Official This category should be used for all personal data, which is not defined as sensitive e.g. Contact Details of Parents, Assessment information etc.	***Schools should mark this as "Official"*** *Some schools will treat anything unmarked as in this category*
Official – Sensitive This category would include any data	***Schools MUST mark this as "OFFICIAL – SENSITIVE"***

deemed to be “Sensitive Personal Data” and access to this should only be on a “Need to Know” basis. Additional security measures may be needed for data in this category.	

Appendix 5 Risk Assessments

Information risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present;
- Judging the level of the risks (both the likelihood and consequences); and
- Prioritising the risks.

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions Form (example below):

Risk ID	***Information Asset affected***	***Information Asset Owner***	***Protective Marking (Impact Level)***	***Likelihood***	***Overall risk level (low, medium, high)***	***Action(s) to minimise risk***
1	*SIMS Data on Pupils*	*Headteacher*	*Official*	*Low*	*Low*	*Ensure Backups Complete* *Ensure Data cleansing completed annually* *Check password compliance*
2	*Safeguarding Information on Individual Pupils*	*Named Safeguarding Person*	*Official Sensitive*	*Low*	*Medium*	*Ensure data passed to agencies is encrypted (email)* *Electronic information stored in a folder with limited, named access* *Paper based information kept locked in…*
3						

Appendix 6 Check Sheet

Schools may find it beneficial to use this to check their systems for handling data.

- Training for staff on Data Protection, and how to comply with requirements
- Data Protection Policy in place
- All portable devices containing personal data are encrypted
- Passwords – Staff use complex passwords
- Passwords – Not shared between staff
- Privacy notice sent to parents
- Privacy notice given to staff
- Images stored securely
- School registered with the ICO as a data controller
- Member of staff with overall responsibility for data identified (SIRO)
- Risk assessments complete
- Systems in place to ensure that data is retained securely for the required amount of time
- Process in place to allow for subject access requests.
- If school has CCTV appropriate policies are in place to cover use, storage and deletion of the data, and appropriate signage is displayed
- Paper based documents secure
- Electronic backup of data both working and secure
- Systems in place to help reduce the risk of a data breach *e.g. personal data sent out checked before the envelope sealed, uploads to websites checked etc*

Appendix 7 Potential Breach Procedure (2015)

Governors and staff are fully committed to the safeguarding of the welfare of all St Joseph's pupils

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

2. 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 stage is to decide whether formal notification of a breach is necessary.

Scope

3. 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
***Sensitive* personal data (as defined by the Data Protection Act 1998)**	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 ▪ Commission or alleged commission of any offence, or ▪ Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings
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
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
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.
ICT Services	Information Communications Technology Services

Legal Context

4. The Data Protection Act 1998 regulates the processing (use) of information relating to living individuals, including the obtaining, holding, use or disclosure of such information.

5. 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?

6. 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 –

  a. at least one of the conditions in Schedule 2 is met, and

  b. in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

- 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.

7. This Data Breach Procedure aims to ensure that the school fulfils the seventh 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.

8. 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.

9. The list is indicative but not exhaustive. If you are, in any way, unsure whether or not a potential breach has taken place legal advice may be sought. Many schools have a legal SLA which may cover appropriate advice.

What about an Information Communication Technology (ICT) breach?

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

Mandatory Procedures

11. 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

12. For each stage, there is **a key decision.** The following steps set out the decision process at each stage.

13. The report template is included as **Appendix 1** to help staff identifying and manage potential breaches.

Reporting the Potential Data Breach:

Headteacher / Senior Information Risks Officer

---

15. **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, you need to start this process.

16. 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.

17. Record the following in the log if known.

a) Date of incident

b) Date you were made aware of the potential breach,

c) Location of incident,

d) Nature of incident, that is, is it a loss, theft, disposal, unauthorised disclosure?

e) Nature of data involved, list all data elements. For example, whether it is names, files, dates of birth, or reference numbers

f) What security protection was on the data? Is it protected by a password, encryption, or something else?

g) Is there a back up of the data, if so where?

h) Number of people potentially affected, an estimate should be provided if no precise figure can be given.

i) 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**

Headteacher **/** **SIRO**

---

20. 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.

21. 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.

22. If the breach has not been contained then the school should follow the data breach investigation template A copy of this template is attached as **Appendix 2**.

23. The Headteacher 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.

24. If a pupil is potentially in danger from the breach, their safety is a priority and they must be protected. Contact the LADO. Once they are safe, then an investigation can commence.

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

25. 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 Breach	**Responsible Officer**
	SIRO / Headteacher / Chair of Governors

26. 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 the LADO may need to be informed.

27. A template for investigating data breaches is attached at the end of the document. The Root Cause Analysis model (RCA) is based upon the NHS's approach to investigating incidents.

28. 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. It may be necessary to notify the LADO of the data loss.

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.

29. 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.

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

Managing the Potential breach **Responsible Officer**

Headteacher / SIRO

---

36. 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?**

37. The primary consideration will be the wellbeing of the people affected by the breach.

38. 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 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?

39. 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.*

40. 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 formal breach**		**Likely to require recommending as a formal breach**	

41. 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, and 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 service. 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 distressed. 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 council 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 / SIRO / Chair of Governors

43. The final evaluation process is done by the Head 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.

44. The School should implement any actions highlighted by the report**.**

Formal Notification of Breaches **Responsible Officer**

Headteacher / Chair of Governors

47. The **fourth decision stage** is whether the data breach was severe enough to require the school to inform the Information Commissioners 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.

Data Breach Investigation Report Template

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

(Please read – instruction for use of this RCA report template)

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, LADO, ICO, Legal Team) in assisting the school in dealing with the consequences of the breach.

Column A **Quick reference guide**	**Column B** **Type your investigation report in this column**
Incident Date	Add 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 individual concerned has been notified to allow them to be vigilant account 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 info recovered if recovered. When data subject informed risk etc.
Contributory factors (A list of significant contributory facts).	Over 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 where ever 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	Example only (please delete and add your own findings)
will be shared with staff and other organisations).	• 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 and Chair of Governors **Date**	