Laurel Avenue
Community Primary School

Data Protection Policy (GDPR Compliant) May 2108

Introduction

Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature.
It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not

- *have permission to access that data, and/or*
- *need to have access to that data.*

Data breaches can have serious effects on individuals and/or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in GDPR legislation and relevant regulations and guidance for the local authority, DfE and ICO.

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 disposed of*
- *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

Article 5 of the GDPR sets out that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, subject to measures respecting the principle of 'data minimisation', not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals, and again subject to the 'data minimisation' principle; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In Addition article 5(2) requires that the controller shall be responsible for, and be able to demonstrate, compliance with the principles. *In effect the school, as the 'data controller', needs to be able to show that its policies and systems comply with requirements of GDPR.*

2. Lawful Basis for processing data

GDPR stipulates that there must be a lawful basis for processing data, and that for special category data an additional condition has to be met. The vast majority of information that schools collect and process is required to enable the school to perform tasks carried out in the public interest or in the exercise of official authority vested in the school, as the data controller. This is the main lawful basis for processing data that a school is likely to rely on.

There are other bases that may be available, such as a specific legal obligation applying to the data controller that makes the processing necessary. Your legal advisor will be able to identify individual statutes if required.

2.1 Age. *Children under the age of 13 are not considered able to give consent to process data or to directly access the rights of a data subject, so parents or guardians do this on their behalf. Over the age of 13 this responsibility is transferred to the child and parents will not have responsibility for their child's data. (This is subject to the Data Protection Bill becoming law. The 'default' age under the GDPR is 16.)*

2.2 Consent. *If there is a lawful basis for collecting data then consent to collect data is not required. (An employee could not opt to withhold an NI number for example.) However, a privacy notice which explains to data subjects (or the parents of the data subject if under the age of 13) will be required. This explains the lawful basis for processing the data, and also explains to the individual their rights.*

Parents/Carers or children over the age of 13 will need to give consent when there is not a legal reason for processing, for instance for images used in school publicity or social media feeds. The consent will need to be transparent, revocable, and will need to be on an "Opt-in" basis.

RIGHTS

The GDPR creates some new rights for individuals and strengthens some existing ones. It provides for the following rights:

1. *The right to be informed*
2. *The right of access*
3. *The right to rectification*
4. *The right to erasure*
5. *The right to restrict processing*
6. *The right to data portability*
7. *The right to object*
8. *Rights in relation to automated decision making and profiling.*

For "privacy notices" covering the right to be informed, please see section 5 below.

Different rights attach to different lawful bases of processing:

	Right to erasure	***Right to portability***	***Right to object***
Vital Interests	✓	***X***	***X***
Legal Obligation	*X*	***X***	***X***
Public Task	***X***	***X***	✓
Legitimate Interests	✓	***X***	✓
Contract	✓	✓	***X***
Consent	✓	✓	*X but right to withdraw consent*

The right to erasure. *GDPR includes a right to erasure – but this is not an absolute right and does not necessarily override the lawful basis for continuing to hold data. Your legal advisor will be able to support with*

information about which data can continue to be legally held if a data subject asks to be 'forgotten'. Schools' data management systems such as SIMS will begin to improve their functionality to either delete or anonymise personal data when appropriate.

It will be seen from the table above that where a school relies on either a 'legal obligation' or a 'public task' basis for processing (see above) there is no right to erasure – however this does not mean the data will never be erased. It will still not be retained for any longer than necessary, in accordance with statutory requirements and/or the school's data retention guidelines.

3. Data Types

Not all data needs to be protected to the same standards - the more sensitive or potentially damaging the loss of 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. GDPR 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, or "special category", personal data is considered much more seriously and the sanctions may well be more punitive.

3.1. 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.*

3.2. Special Category Data

"Special Category Data" are data revealing a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data, data concerning a person's health or sexual life is prohibited except in special circumstances.

This is because special category data is more sensitive, and so needs more protection.

In a school the most likely special category data is likely to be:

- *information on the racial or ethnic origin of a pupil 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 (SEND)*
- *(Some information regarding safeguarding will also fall into this category.)staffing e.g. Staff Trade Union details*

Note – See section on sharing information.

3.3. 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 publicly (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 provides additional information on their website. See http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions

4. Responsibilities

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

4.1. Risk Management – Roles: Data Protection Officer

The school should have a nominated member of staff responsible for the management of data protection.

According to the ICO the minimum role will include:

- *to inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws*
- *to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits*
- *to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).*

In some schools other staff may have been delegated responsibility for particular issues, for instance the handling of SEND information.

The school will identify these as Mrs J Ferguson, Admin Officer; Mrs M Angus, Admin Officer; Ms G Davison, Headteacher (SENCO) for the various types of data being held (e.g. pupil information/staff information etc.).

The DPO and persons with delegated responsibility 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*

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

4.2. 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 to personal data, when engaged in their role as a Governor.*

4.2.1 Risk Assessments

Information risk assessments will be carried out by the DPO at the time of implementation of GDPR for all current systems and on the introduction of new systems, 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 on-going process and should result in the completion of an entry in the Information Asset Register:

Type of data	What personal data is stored?	How is it collcete d	Basis for Collectio n	Includes Special category data	Where is the data stored?	Is it held by a third party?	Is a GDPR - compliant contract in place with the third party?	Security Measures - Access Control	Who has access to it?	Is it ever taken off-site?	Shared wi

4.2.2 Impact Levels and protective marking

Following incidents involving loss of data, the Government published HMG Security Policy Framework [http://www.cabinetoffice.gov.uk/spf], which recommends that the Government Protective Marking Scheme is used to indicate the sensitivity of data.

The HMG Security Policy recommends that the Government Protective Marking Scheme is used to indicate the sensitivity of data. The scheme is made up of five markings, which in descending order of sensitivity are: TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED and PROTECT. Most learner or staff personal data that is used within educational institutions will come under the PROTECT or RESTRICTED classifications.

To ensure a uniform method of assessing the impact of potential compromises to the confidentiality, integrity or availability of information and information systems, and provide comparable levels of information protection when the data is shared, Business Impact Levels tables have been devised. All data – electronic or on paper – should be labelled according to the protection it requires, based on these Impact Levels. Impact Levels 2 -6 correspond to the adjectival descriptions PROTECT to TOP SECRET.

The following table illustrates the assignation of Impact Levels for Distress to the Public.

Impact Level 1	***Impact Level 2***	***Impact Level 3***	***Impact Level 4***
Not Protectively Marked	*Protect*	*Restricted*	*Confidential**
None	*Likely to cause embarrassment to an individual or organisation*	*Likely to cause loss of reputation to an individual or organisation*	*Likely to cause embarrassment or loss reputation to many citizens or organisatio*

**Confidential, Secret and Top Secret are not applicable in a school setting*

Impact Level	***Example Data Types***
IL0/IL1	• *Google search results* • *BBC News*
IL2 – PROTECT	• *General student data* • *Learning platforms/portals*
IL3 – RESTRICTED	• *School MIS (eg SIMS data)*

Impact Level	*Example Data Types*
	• *Teacher access to learning platform/p* • *Special educational needs* • *Pupil characteristic* • *Health records*
IL4 - CONFIDENTIAL	• *National Pupil Database* • *Looked-after children* • *Witness protection* • *SEN IL4 data elements*

The person writing a document is responsible for applying the correct protective marking. They do this by clearly labelling each page of a document, normally in the footer, with the correct marking.

When protectively marking a document, it is recommended that a damage or 'harm test' is conducted to consider the likely impact if the asset were to be compromised and to help determine the correct level of marking required.

If applied correctly, the Protective Marking System will ensure that only genuinely sensitive material is safeguarded. Be aware that applying too high a protective marking can inhibit access and impair efficiency while applying too low a protective marking may lead to damaging consequences and compromise of the data.

Most pupil or staff personal data that is used within educational institutions will come under the PROTECT classification. However some, e.g. the home address of a child (or vulnerable adult) at risk will be marked as RESTRICT.
The school will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to and the handling and storage of data classified as Protect, Restricted or higher.
Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

Users must be aware that when data is aggregated, the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts pupils at serious risk of harm will have a higher impact than a risk that puts them at low

risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer e.g. 'Securely delete or shred this information when you have finished using it'.

4.3 Training and Awareness

All staff will receive data handling awareness/data protection training and will be made aware of their responsibilities, as described in this policy through:

- *Induction training for new staff*
- *Staff Meetings/Professional Development Sessions*
- *Day to day support and guidance from DPO*

5. Legal Requirements

5.1. 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

5.2. Information for Data Subjects (Parents, Staff): PRIVACY NOTICES

*In order to comply with the fair processing requirements of the DPA, the school **must** 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, the legal basis for holding it and the third parties (e.g. LA, DfE, etc) to whom it may be passed. The privacy notice will also need to set out the data subjects' rights under the GDPR. 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*

*New privacy notices should be issued to all 'data subjects' by May 2018 even if the data subject has previously received a similar notice. This is because of the new rights in the GDPR that people should be informed about. (see school **Privacy Notice May 2018**)*

6. Transporting, Storing and Disposing of personal Data

6.1. Information security - Storage and Access to Data

The more sensitive the data the more robust the security measures will need to be in place to protect it.

6.1.1. 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. (see school policy: **Password Security**)*

(http://fluencycontent2-schoolwebsite.netdna-ssl.com/FileCluster/LaurelPrimarySchool/MainFolder/Policies/School-Password-Security-Policy-2018.pdf)

- *All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.*

*(see school policy: **Secure storage of and Access to Data Policy**)*

*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. (see school policy: **Secure Storage of and Access to Data Policy**)*

*The school / academy has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups. (see school policy**: Automatic Backup Systems**)*

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*
- *the school will need to set its own policy as to whether data storage on removal media is allowed, even if encrypted – some organisations do not allow storage of personal data on removable devices*
- *Only encrypted removable storage purchased/approved by the school is allowed to be used on school computers and these are not functional with scanners.*

*(see school policy: **Portable Devices and Removable Media Section of Secure storage of and Access to Data Policy**)*

6.1.2. 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. (see school policy: **Password Security**)*
(http://fluencycontent2-schoolwebsite.netdna-ssl.com/FileCluster/LaurelPrimarySchool/MainFolder/Policies/School-Password-Security-Policy-2018.pdf)

6.1.3. Images

- *Images of pupils will be collected, stored and shared in accordance with the School Photographic Policy and, Secure Storage and Cloud Based Systems Policies.*
- *(see school policy: **School Photographic Policy**) LINK WILL BE ADDED*

6.1.4. Cloud Based Storage

- *The school / academy has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example Dropbox, Google Apps and Onedrive) 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. See advice from the DfE below:-*
- *https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act*

6.2 Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- *Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location*
- *Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school*
- *When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home),they should have secure remote access to the management information system or learning platform, Durham Learning Gateway*
- *If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location*
- *Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and particular care should be taken if data is taken*

or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event. (nb. to carry encrypted material is illegal in some countries)

6.3 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 as well as data processing agreements.
http://ico.org.uk/for_organisations/data_protection/topic_guides/data_sharing

6.4 Retention of Data

Retention of data under GDPR requires an increased emphasis on data minimisation depending upon the data item and justification for retention.

- *The guidance given by the Information and Records Management Society – Schools records management toolkit will be used to determine how long data is retained.*

*(See **School Records Management Policy**)*

Systems to protect data

6.4.1 Paper Based Systems

- *All paper based personal data will be protected by appropriate controls, for example:*
  - *Paper based safeguarding chronologies will be in a locked cupboard when not in use*
  - *Class Lists used for the purpose of marking may be stored in a teacher's bag.*
- *Paper based personal information sent to parents (will be checked by …, before the envelope is sealed).*
- *Passwords are used to secure print jobs of data such as performance data and all special category data, for example SEND, Medical.*

6.4.2 School Websites

- *Uploads to the school website will be checked prior to publication, for instance:*
  - *to check that appropriate photographic consent has been obtained*
  - *to check that the correct documents have been uploaded.*

6.4.3 E-mail

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

- *Where technically possible all e-mail containing sensitive information will be encrypted by (... for instance ... by attaching the sensitive information as a word document and encrypting the document / compressing with 7 zip and encrypting. The recipient will then need to contact the school for access to a one-off password) or*

6.4.4 Admin and Curriculum Servers

All data should be backed up according to its value to the Institution, the cost of recreating the data, any financial costs or penalties which might be incurred as a result of data loss or corruption, and the risk of data loss or corruption.

The purpose of data backup is purely to allow the Institution to continue its activity after a data loss incident, by retrieving some or all of the data lost, ideally from a point in time backup taken within the last 24 hours.

The school has clear policy and procedures for both the protection against virus and other threats including the use of PANDA anti-virus software and automatic backing up, accessing and restoring all data held on school systems, both on and off-site. backups. (see ***Automatic Backup Systems Policy****)*

6.4 Disposal of Data

- *The school will comply with the requirements for the safe destruction of personal data when it is no longer required.*
- *The disposal of <u>personal</u> data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government*

guidance, and other media must be shredded or otherwise disintegrated for data.

- *A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.*

7 Data Sharing

The school is required by law to share information with the LA and DfE. Further details are available at:
https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data

Durham LSCB also provides information on information sharing at:
http://www.durham-lscb.org.uk/wp-content/uploads/sites/29/2016/06/Guide-for-professionals-on-information-sharing.pdf

Schools should ensure that, where special category data is shared, it is transmitted securely for instance by secure e-mail such as Egress or is transferred in tamper proof envelopes securely delivered to the recipient.

8 Freedom of Information Act

Laurel Avenue Community Primary School has a Freedom of Information Policy which sets out how it will deal with FOI requests. In this policy the school should:

- *Delegate to the Headteacher day-to-day responsibility for FOIA policy and the provision of advice, guidance, publicity and interpretation of the school's policy.*
- *Consider designating an individual with responsibility for FOIA, to provide a single point of reference, coordinate FOIA and related policies and procedures, take a view on possibly sensitive areas and consider what information and training staff may need.*
- *Consider arrangements for overseeing access to information and delegation to the appropriate governing body.*
- *Proactively publish information with details of how it can be accessed through a Publication Scheme and review this annually.*

- *Ensure that a well-managed records management and information system exists in order to comply with requests.*

(see school policy: ***Freedom of Information****)*
http://fluencycontent2-schoolwebsite.netdna-ssl.com/FileCluster/LaurelPrimarySchool/MainFolder/Content/Documents/Policies/Freedom-of-Information-2017.pdf

9 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 data protection officer will inform the head teacher and chair of governors.*
- *The school will follow the procedures set out in Appendix 5.*

10 Policy Review Reviewing:

This policy will be reviewed, and updated if necessary every two years or when legislation changes.

Date: *Review:*

Signed:
Chair of Governors

Adopted by the Governing Body on _____

The Data Protection Officer is Mrs Helen Walters (Deputy Headteacher)

Appendix 1 - Links to resources and guidance

ICO Guidance on GDPR

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr

http://ico.org.uk/for_organisations/sector_guides/education

Specific information for schools is available here. This includes links to guides from the DfE

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

Specific Information about CCTV

Information and Records Management Society – Schools records management toolkit

http://irms.org.uk/page/SchoolsToolkit

A downloadable schedule for all records management in schools

Disclosure and Barring Service (DBS)

https://www.gov.uk/government/publications/handling-of-dbs-certificate-information/handling-of-dbs-certificate-information

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-of-children-in-schools

Appendix 2 - Privacy Notices

These are now a separate attachment

Appendix 3 - Glossary

GDPR - The General Data Protection Regulation. *These are new European-wide rules that are the basis of data protection legislation. They are enforced in the UK by the ICO.*

Data Protection Act 1998: Now superseded by GDPR

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 and GDPR

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.

52. ***Appendix 4 - Check Sheet***

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

- ☐ *Data protection Officer in place*
- ☐ *Information asset log complete*
- ☐ *School able to demonstrate compliance with GDPR*
- ☐ *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/pupils aged 13 or over*
- ☐ *Privacy notice given to staff*
- ☐ *Images stored securely*
- ☐ *School registered with the ICO as a data controller*
- ☐ *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*

DATA PROTECTION POLICY Potential Breach

Procedure

Appendix 5

2018

DATA PROTECTION POTENTIAL BREACH PROCEDURE

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 stages are to decide whether notification of a breach to either the data subjects or the ICO 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

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.
GDPR	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 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 GDPR) that may be relevant:	(i) explicit consent (ii) necessary processing by an employer (iii) to protect vital interests (iv) where the data has been manifestly made public by the subject

	(v) necessary for judicial proceedings (vi) necessary for substantial public interest reasons (vii) necessary health processing (viii) necessary for archiving purposes
Actionfraud	http://www.actionfraud.police.uk/ National cybercrime reporting centre.
ICT School Services	ICTSS 03000 261100

Legal C ontext

4. The Data Protection Act regulates the processing (use) of information relating to living individuas, 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 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.

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 a 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. (See also the flowchart at end of document.)

13. The report template is included (at the end of the documentto help staff identifying and manage potential breaches.

Reporting the Potential Data Breach **Responsible Officer**

Headteacher / Data protection officer

---

14. **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.

15. 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.

16. 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 / Data protection officer

17. 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.

18. 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'.

19. 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.
20. 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.

21. **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?

22. 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 Data protection officer / Headteacher / Chair of Governors

23. 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.

24. 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.

25. 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.

26. 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.

27. 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.

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

Managing the Potential Breach	Responsible Officer
	Headteacher / Data protection officer

29. 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?**

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

31. 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?

32. 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.*

33. 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**	

34. 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

35. 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.

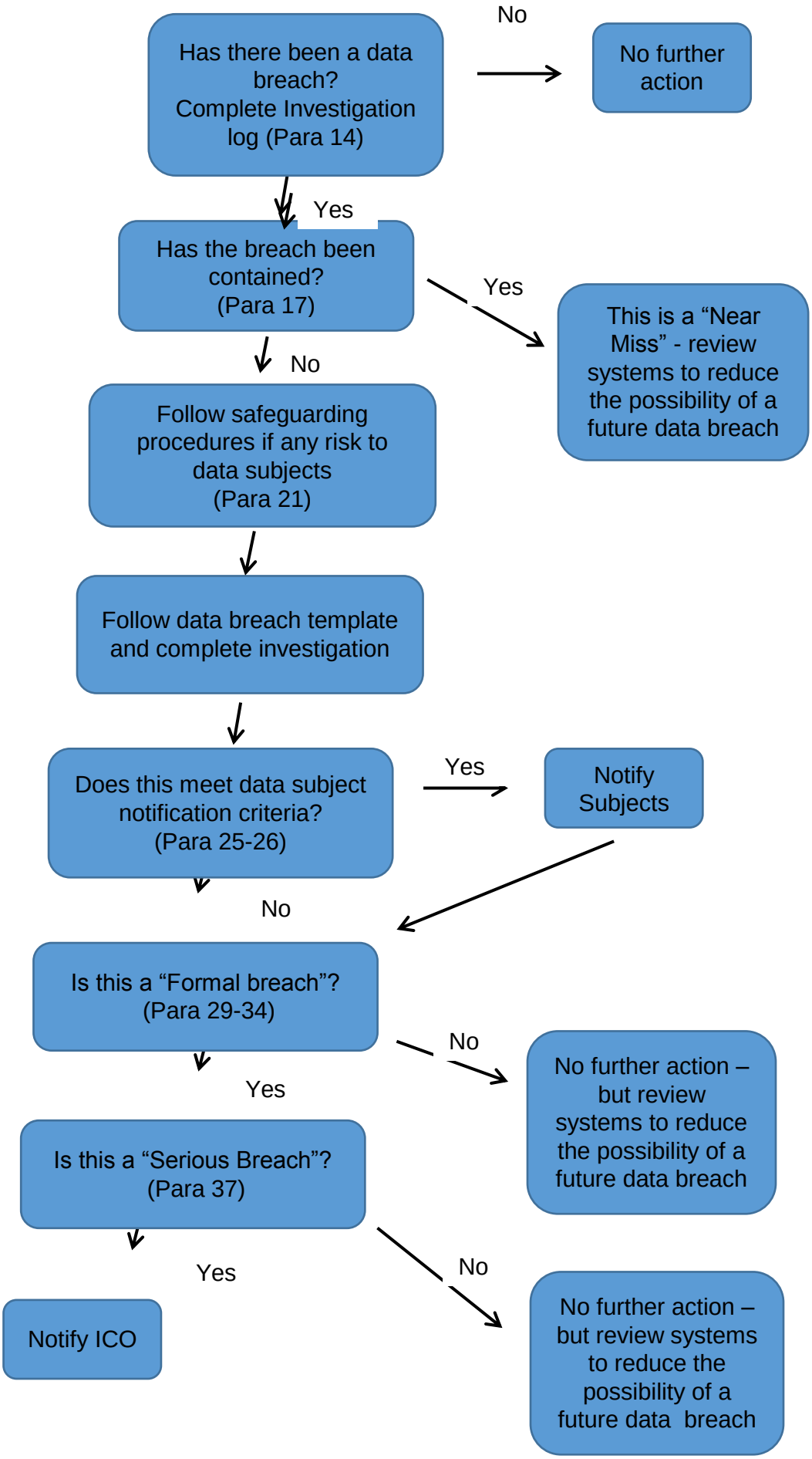
36. The school should implement any actions highlighted by the report.

Formal Notification of Breaches	Responsible Officer
	Headteacher / Chair of Governors

37. 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



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

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

1. **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.

2. **Once you have completed column B, you need to delete column A. * <u>All that is required is column B</u>***

   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 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. **Chronology of events** (For complex cases any summary timeline included in the report should be a summary.)	*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. 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.) **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.)	Over the years email addresses had been added, causing the team to lose track of the internal and external lists. 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.) **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)* • Share findings with other schools sharing similar activities. • Share findings to identify opportunities for sharing outside the organisation. *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	