Data Protection Policy Northwick Park Academy Trust

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

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.

1.3. Our Commitment:

The Northwick Park Academy Trust is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and the Data Protection Act (DPA).
https://ico.org.uk/for-organisations/guide-to-data-protection/data-protectionprinciples/
Changes to data protection legislation (GDPR May 2018) shall be monitored and implemented in order to remain compliant with all requirements.

The legal bases for processing data are as follows –

(a) Consent: the member of staff/student/parent has given clear consent for the school to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for the member of staff's employment contract or student placement contract.

(c) Legal obligation: the processing is necessary for the school to comply with the law (not including contractual obligations)

The members of staff responsible for data protection are mainly Emma Lane (Head Teacher), Tracy Smith (Acting Deputy Head Teacher) and Sarah Coulson (Academy Finance Officer), Elaine Rising and Sharon Rosher (ICT technicians).
However all staff must treat all student information in a confidential manner and follow the guidelines as set out in this document.
The school is also committed to ensuring that its staff are aware of data protection policies, legal requirements and adequate training is provided to them through our academy training service.
The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

1.4. Notification:

Our data processing activities will be registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller. Details are available from the ICO:
https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/
Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.
Breaches of personal or sensitive data shall be notified within 72 hours to the individual(s) concerned and the ICO.

1.5. Personal and Sensitive Data:

All data within the school's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.
The definitions of personal and sensitive data shall be as those published by the ICO. For guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/keydefinitions/
The principles of the Data Protection Act shall be applied to all data processed:

- ensure that data is fairly and lawfully processed
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive
- ensure that data processed is accurate
- not keep data longer than is necessary

- process the data in accordance with the data subject's rights
- ensure that data is secure
- ensure that data is not transferred to other countries without adequate protection.

2. 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. The DATA PROTECTION ACT 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, 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 progress records, reports, references
- Professional records e.g. banking details, 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 including health and social care.

2.2. Sensitive Personal data

Sensitive personal data is defined by the Act as information that relates to: race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexual life and biometric data. 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 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
- Some information regarding safeguarding will also fall into this category.

Note – See section on sharing information.

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 DATA PROTECTION ACT - 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 provides additional information on their website. See
http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions

2.4. Fair Processing / Privacy Notice:

We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and pupils prior to the processing of individual's data.
Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.
https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-noticestransparency-and-control/

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities, for example local authorities, Ofsted, or the department of health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.
The intention to share data relating to individuals to an organisation outside of our school shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.
Any proposed change to the processing of individual's data shall first be notified to them.
Under no circumstances will the school disclose information or data:

- that would cause serious harm to the child or anyone else's physical or mental health or condition
- indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child
- recorded by the pupil in an examination
- that would allow another person to be identified or identifies another person as the source, unless the person is an employee of the school or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed

- in the form of a reference given to another school or any other place of education and training, the child's potential employer, or any national body concerned with student admissions.

3. Responsibilities

The Head teacher and Governing Body are responsible for Data Protection, they should appoint a Data Protection Officer to manage data. The Data Protection Officer for the Northwick Park Multi Academy Trust is IGS – Information Governance Support with Essex County Council. This is supported in each school by Elaine Rising (Northwick Park) and Tracy Smith (Leigh Beck)

3.1. Risk Management – Roles:

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).
- Within the Northwick Park Academy Trust, the SENCO information is held by the SENCo and shared with class teachers as necessary – sensitive information will be held safely and securely.

3.2. Data Security:

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them.
Risk and impact assessments shall be conducted in accordance with guidance given by the ICO:
https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/
https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2014/02/privacyimpact-assessments-code-published/

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.
The security arrangements of any organisation with which data is shared shall also be considered and where required these organisations shall provide evidence of the competence in the security of shared data.

3.3. Data Access Requests (Subject Access Requests):

All individuals whose data is held by us, has a legal right to request access to such data or information about what is held. We shall respond to such requests within one month and they should be made in writing to:

Mrs Emma Lane
Northwick Park Academy Trust
Third Avenue
Canvey Island
Essex SS8 9SU

No charge will be applied to process the request.

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 to 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 DATA PROTECTION ACT, the school will inform parents / carers of all pupils and staff of the data they collect, process and hold on the pupils , the purposes for which the data is held and the third parties (e.g. LA, DfE, Target Tracker etc) to whom it may be passed. This privacy notice will be passed to parents / carers through a letter.

See Appendix 2.

5. Transporting, Storing and Disposing of personal Data

The policy and processes of the school will comply with the guidance issued by the ICO and are supported by IGS.

5.1. 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.
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

Schools should ensure that, where data that is shared, it is transmitted securely for instance by secure e-mail.

Location of information and data:
Hard copy data, records, and personal information are stored out of sight and in a locked cupboard. The only exception to this is medical information that may require immediate access during the school day. This will be stored with the school medical coordinator.
The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:
• Paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.
• Unwanted paper copies of data, sensitive information or pupil files should be shredded or sent for confidential disposal. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.
• Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.

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.
- 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. (The school will need to set its own policy, relevant to its physical layout, type of ICT systems etc. Schools need to be aware of a significantly higher risk of a data loss, and should ensure that they can recover from a cyber-attack.)

5.1.2. Portable Devices

Sensitive or personal information and data should not be removed from the school site, however the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with pupils.
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. Staff are issued with encrypted USB sticks to store necessary data on for work purposes when away from school
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete. Staff will return USB sticks to school to be checked on request. The data should not be transferred from this stick onto any home or public computers. Work should be edited from the USB, and saved onto the USB only.

5.1.3. Data Sharing

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. Data may be disclosed to the following third parties without consent:

• **Other schools**
If a pupil transfers from a Northwick Park Academy Trust school School to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.

• **Examination authorities**
This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

• **Health authorities**
As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

• **Police and courts**
If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

• **Social workers and support agencies**
In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

• **Educational division**
Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

• **Right to be Forgotten:**
Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the school including any data held by contracted processors.

5.1.4. Passwords

All users will use strong passwords which must be changed regularly for school email addresses – every 90 days. User passwords must never be shared. It is advisable NOT to record complete passwords, but prompts could be recorded. These prompts will be held by the ICT technician team, in both schools, on encrypted memory sticks and locked into the safe.

5.1.5. Images

Images of pupils will only be processed and transported by use of staff and permission for this will be obtained in the fair processing notice. Parents will be asked to give permission for photographs and video to be taken by school staff both within school and at school events and for those photographs and videos to be displayed around school, where they can be seen by visitors to the school, and used in work and assessments, including for those children with SEND, within the classes and school as a whole. Parents will also have to give permission of children's photographs to be used on the school or Trust websites.
Staff will only store images on the secure school drives and if included in reports on encrypted USB drives.

5.1.6. Cloud Based Storage

The school has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example 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. All cloud based storage providers will have to comply with the GDPR procedures before the school will consider access to these. Certificates for these will be verified by the Data Protection Officer(s)

See advice from the DfE below:-
https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act

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 as well as data processing agreements.
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 personal data will be protected by appropriate controls, for example:

- Paper based safeguarding chronologies will be in a locked cabinet when not in use and the key will also be stored away from the cabinet in a locked drawer
- 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 the School Operations Manager, before the envelope is sealed).

5.4.2. 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.

5.4.3. 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. This may be sent in a separate email once confirmation of the original document has been received by the recipient.

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

6. 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 who will liaise with the chair of governors and Trust Directors.

The school will follow the procedures set out in Appendix 7.

Data Disposal:
The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.
All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.
All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

Disposal of IT assets holding data shall be in compliance with ICO guidance:
https://ico.org.uk/media/fororganisations/documents/1570/it_asset_disposal_for_organisations.pdf
The school has identified a qualified source for disposal of IT assets and collections – PRM Green Technologies (level 5 approved)
The school also uses Shred4Security to dispose of sensitive data that is no longer required.

7. Policy Review Reviewing:

This policy will be reviewed, and updated if necessary every two years or when legislation changes. GDPR is due to be implemented in May 2018.

Date:

Review:

Signed:
Chair of Governors

Adopted by the Governing Body on _____

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

Specific information for schools is available here
http://ico.org.uk/for_organisations/data_protection/topic_guides/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 (May 2016)

The templates below are taken from the DFE website at:
https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices

ADDITIONAL WORDING AND LA LINKS
LA
Links to LA Information
https://schools-secure.essex.gov.uk/data/information-governance/Pages/default.aspx
InformationGovernanceSupport@essex.gov.uk

ADDITIONS
Text Service (Some schools use a commercial texting service to contact parents)
The school uses a texting service managed by Teacher's to Parents to communicate with parents. Please contact Mrs Smith for further information or if you want to opt out of this arrangement.

Privacy Notices:
DfE may also share pupil level personal data that we supply to them with third parties. This will only take place where legislation allows it to do so and it is in compliance with the Data Protection Act 1998.
Decisions on whether DfE releases this personal data to third parties are subject to a robust approval process and are based on a detailed assessment of who is requesting the data, the purpose for which it is required, the level and sensitivity of data requested and the arrangements in place to store and handle the data. To be granted access to pupil level data, requestors must comply with strict terms and conditions covering the confidentiality and handling of data, security arrangements and retention and use of the data.
For more information on how this sharing process works, please visit:
https://www.gov.uk/guidance/national-pupil-database-apply-for-a-data-extract

For information on which third party organisations (and for which project) pupil level data has been provided to, please visit: https://www.gov.uk/government/publications/national-pupil-database-requests-received

The DfE website
 https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

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 either 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 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.	Schools MUST mark this as "OFFICIAL – SENSITIVE"

DATA PROTECTION POLICY Potential Breach Procedure

Appendix 7

DATA PROTECTION POTENTIAL BREACH PROCEDURE

Sections that have changed from an earlier version are highlighted in green

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
Sensitive personal data (as defined by the Data Protection Act 1998 and/or the emerging GDPR)	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.

DATA PROTECTION ACT	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 DATA PROTECTION ACT)
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.
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 Context

4. The Data Protection Act 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 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. Contact IGS for in school support, via the members of staff responsible for Data Protection within school who will inform the Head Teacher and decide the appropriate course of action.

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 document to help staff identifying and manage potential breaches.

Reporting the Potential Data Breach

Responsible Officer Head teacher / 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 Head teacher 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/Board of Directors.

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 Head teacher / Data protection officer / 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 Head teacher / 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 Head teacher / Data protection officer / Chair of Governors

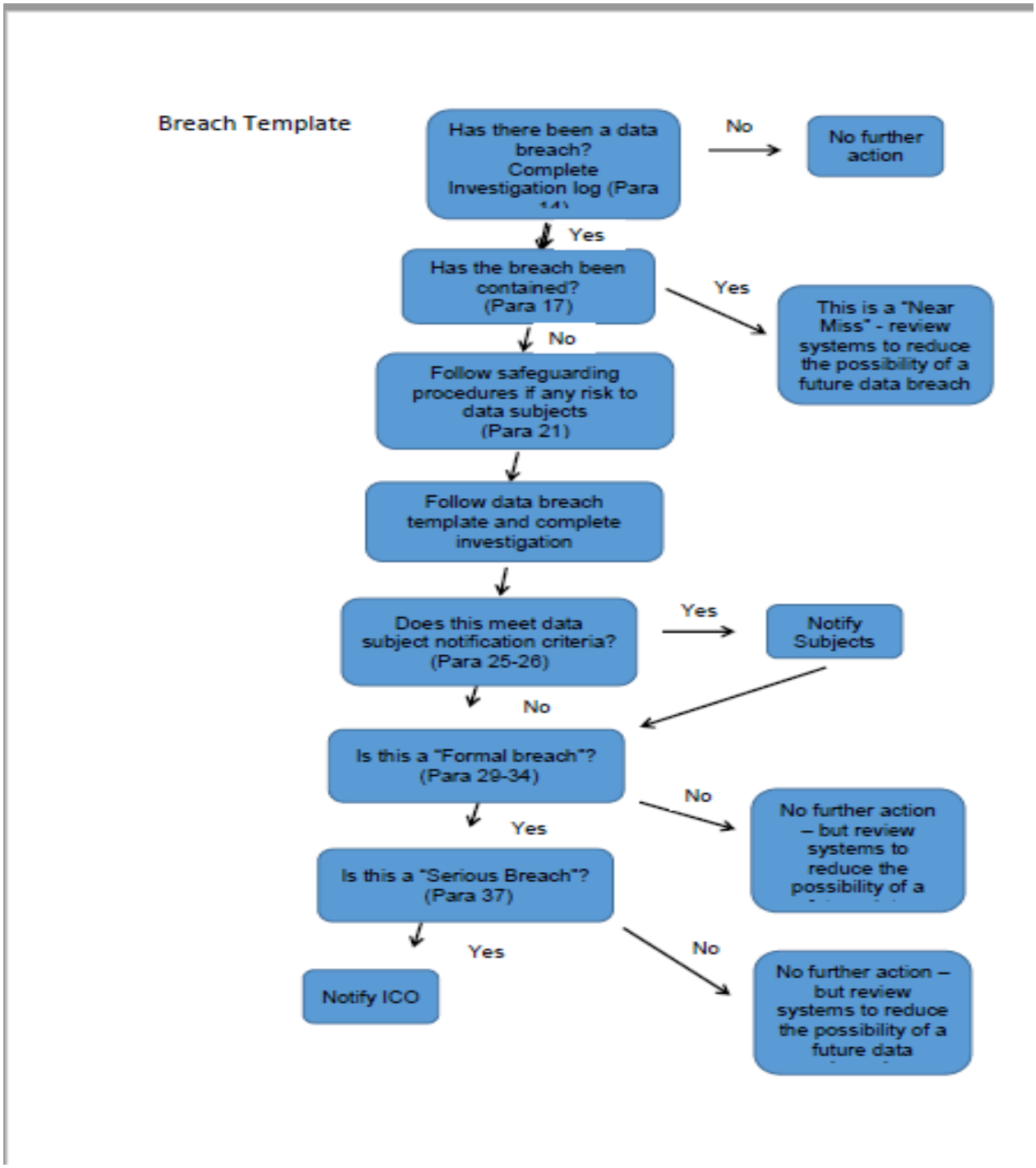
35. The final evaluation process is done by the Head and Governing Body to consider the causes of the breach and the lessons that need to be learned. The investigation report indicates how effective the school was in response to the breach. The school should also seek advice from the School and Governor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

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

Formal Notification of Breaches

Responsible Officer Headteacher / Data protection officer / 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.



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.

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

If issues arise which require a new heading this can be added as a new row.
Once you have completed column B, you need to delete column A. * All that is required is column B*

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

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

Column A	Column B
Quick reference guide	Type your investigation report in this column
Incident Date	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 individuals concerned have been notified to allow them to be vigilant for any suspicious activity on their account.
Chronology of events (For complex cases any summary timeline included in the report should be a summary.)	The key points of the event: when discovered, when last use of data, when authority notified, when information recovered if recovered, when data subject informed of risk etc.
Contributory factors (A list of significant contributory facts.)	Over the years email addresses had been added, causing the team to lose track of the internal and external lists

Root Causes (These are the most fundamental underlying factors contributing to the incident that can be addressed. Root causes should be meaningful (not sound bites such as communication failure) and there be a clear link, by analysis, between root CAUSE and EFFECT.)	Staff involved have not had training on use of internal and external lists. Internal and external lists have names that are only different by one letter. There is no procedure for creating distributions lists to be used by service.
Lessons learned (Key issues identified which may not have contributed to this incident but from which others can learn.)	The external lists should be marked clearly and consistently as external
Type of breach	Please tick one of the following: Near miss ☐ Potential breach ☐ Further action: ☐ *please provide details* No further actions ☐ Formal breach ☐
Recommendations (Numbered and referenced) Recommendations should be directly linked to root causes and lessons learned. They should be clear but not detailed. (Detail belongs in the action plan.) It is generally agreed that key recommendations should be kept to a minimum 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 will be shared with staff and other organisations.)	Example only (please delete and add your own findings) • Share findings with other schools sharing similar activities. • Share findings to identify opportunities for sharing outside the organisation.
Outcome (The conclusion of the investigation should state whether the author believes the breach should be logged formally or not.)	Example only (please delete and add your own findings) As the breach resulted in sensitive personal information being inappropriately shared with more than 10 people, it is recommended that this be recorded as a formal data breach.
Head teacher and Chair of Governors Date	