Our Lady and St Joseph Catholic Primary School

INFORMATION GOVERNANCE POLICY

Prepared by: Lucy Henderson and Naomi Korn Associates
Approved by: Governing Body
Date: Feb 2022
Review Date: Feb 2023
Checked DPO: Feb 2022

INDEX

1. Introduction to Information Governance

1.1 This document constitutes Our Lady and St Joseph Catholic Primary School's Information Governance Policy. It details the School's obligations and compliance with relevant legislation in relation to its handling of data. It also sets out the School's commitment to providing appropriate training and increasing awareness in this area.

1.2 This Policy pulls together all the requirements for information governance so that all School information is processed legally, securely, efficiently and effectively. Information plays a key part in the School's day to day operations and governance. Accordingly, this Policy sets out the requirements, standards and best practice that apply to the handling of all information.

1.3 Information governance is a key responsibility of each and every member of the School's community. It is essential that School staff and Governors/Trustees familiarise themselves with this Policy and the attached appendices. This Policy and the governance it sets, are also expected of any third parties handling School information.

1.4 The aim of this Policy is to support the school to:

- comply with its legal, regulatory and contractual obligations;
- maintain robust corporate governance and deliver high quality education;
- deliver value for money and protect the public funds;
- improve the way the School handles, utilises and protects its information;
- increase the School's openness, transparency and engagement with the general public;

1.5 The School holds and processes Standard and Special Category Data (as described in **2.3** below) for the purposes of education provision, performance monitoring, commercial engagement, contractual obligations, research and the safeguarding.

2. Scope

2.1 This Policy covers all information held by the School or on behalf of the School whether in electronic or physical format including (but not limited to):

- Electronic data stored on and processed by fixed and portable computers and storage devices;
- Data transmitted on networks;
- All paper records;
- Visual and photographic materials including slides and CCTV;

2.2 The following are expected to comply with the Policy:

- All staff and governors/trustees of the School;
- Any third parties handling, or having access to, school information including for example consultants, service providers, contractors, visitors and volunteers.

2.3 The following is the classification template in accordance with which most school data can be classified:

2.3.1 Personal data - this is defined in Article 4 of the General Data Protection Regulation as any information relating to an identified or identifiable natural person (referred to as a 'data subject'), where an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. The collection, use and retention of personal data must comply with strict conditions and such data requires special measures of protection as more particularly described in the School's Data Protection Policy;

2.3.2 Sensitive personal data (also known as special categories of data) is a subset of personal data - this is defined in Article 9 of the General Data Protection Regulation as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data. Medical research data for example is likely to include some sensitive personal data. The processing of Special Category Data is subject to additional requirements and requires additional protections, also as described in more detail in the School's Data Protection Policy;

2.3.3 Criminal Conviction Data – A note of DBS number will be made. Information relating to criminal convictions will only be held, and processed where there is legal authority to do so.

2.3.4 Non-personal data (organisational data) which can be:

- Sensitive organisational data, which includes commercially sensitive planning/administrative or research data, data protected by confidentiality agreements, legally privileged information, etc. This data should be protected by appropriate protection measures; and
- Non-sensitive organisational data which is data pertaining to School not published by default, but which may be disclosed (subject to legal advice) in response to requests made under the Freedom of Information Act.

3. INFORMATION GOVERNANCE STRATEGY

3.1 Purpose

3.1.1 The aim of this document is to enable the School to meet its information management and security responsibilities so that customers, businesses, partners and suppliers have the confidence that information is handled and stored with due regard to its value and risk. Individuals must understand the importance of using information correctly, of sharing it lawfully and of protecting it from improper use.

3.1.2 The intention of this strategy is also to enable the School to meet its legal and ethical obligations in terms of:

- The use and security of personal data;
- Appropriate disclosure of information when required;
- Regulatory Policies for the management of information;
- Professional codes of conduct for consent to the recording, sharing and uses of information;
- Operating procedures and codes of practice adopted by the School;
- Information exchanged with third parties.

3.1.3 The strategy recognises the high standards expected of the School as well as the ongoing task of maintaining appropriate standards of security in the area of information governance and of embedding a security culture fully throughout the School.

3.2 Strategic objectives

3.2.1 These are the overarching information governance objectives of the School. We want the infrastructure and processes for service delivery to provide the right information to the right people at the right time for the right purpose and promote the provision of high-quality services by promoting the ethical, legal, effective and appropriate use of information:

- To promote information governance ensuring that it is, embedded throughout the school and to direct cultural change so that information is regarded as a key asset;
- To build into staff competencies and job descriptions specific requirements around the governance of information;
- To encourage staff to work closely together, preventing duplication of effort and enabling more efficient use of resources;
- To work to achieve required standards to comply with legislative, regulatory and contractual obligations and relevant policies;
- To identify and manage information assets across School;
- To implement and operate proportionate controls that apply best practice standards to protect information assets and give confidence to all interested parties;
- To provide adequate training to all staff, increase awareness and embed a culture of care and responsibility in the handling of all information throughout the School.

3.3 Approach

3.3.1 Information governance and assurance are, integrated into all aspects of School operations. In delivering information governance services, four key elements of School operations will, be considered:

- People
- Process

- Information
- Technology

3.3.2 All information governance, improvement and assurance activities will consider how these factors need to operate in combination to achieve our strategic objectives.

3.4 Benefits

3.4.1 The following benefits (which are not an exhaustive list) provide an overview of the main benefits that, should be derived through the delivery of this strategy:
- Consistent and effective management of information across the School;
- Increased understanding of and compliance with relevant legislation;
- Reduced number of information security incidents;
- Reduced staff time and effort;
- Improved data quality;
- Clear responsibilities in relation to Information Governance and Assurance;
- Effective management of information risks;
- Greater confidence that information risks are effectively managed;

3.5 Governance

3.5.1 The School Governors/Trustees along with the Head Teacher are responsible for implementing this policy.

4. Policies

4.1 This Information Governance Policy incorporates the following individual policies:
- Data Protection Policy
- Breach Policy
- Retention Policy
- Freedom of Information Policy
- Information Asset Register

5. Training and development

5.1 Information governance training and development is essential for the development and improvement of staff knowledge and skills relating to information governance across the School.

5.2 Information governance training must extend beyond basic confidentiality and security awareness in order to develop and follow best practice. Staff must understand the value of information and their responsibility for it, which includes data quality, information security, records management, confidentiality, etc.

5.3 Information governance basic awareness is a mandatory requirement for all new staff as part of their induction.

6. Data Protection

6.1 Our Lady and St Joseph Catholic Primary School collects and uses certain types of personal information about staff, pupils, parents and other individuals who come into contact with the

school in order provide education and associated functions. The school may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding, and this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation and other related legislation.

6.2 GDPR applies to all computerised data and manual files if they come within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured in some way that it is searchable on the basis of specific criteria (so you would be able to use something like the individual's name to find their information), and if this is the case, it does not matter whether the information is located in a different physical location.

7. Personal Data

7.1 The School is the Data Controller for personal data (as defined in 2.3.1) and special category data (as defined in 2.3.2)

7.2 Information relating to criminal convictions will only be held, and processed where there is legal authority to do so.

7.3 Our Lady and St Joseph Catholic Primary School does not intend to seek or hold sensitive personal data about staff or students, except where the School has been notified of the information, or it comes to the school's attention via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice. Staff, Parents/ Carers, Students and Governors/Trustees are under no obligation to disclose to the school their race or ethnic origin, political or religious beliefs, whether or not they are a trade union member or details of their sexual life (save to the extent that details of marital status and / or parenthood are needed for other purposes, e.g. pension entitlements).

8. The Data Protection Principles

8.1 The six data protection principles as laid down in the GDPR, are followed, by the School at all times:

- processed lawfully, fairly and in a transparent manner in relation to the data subject
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- 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;
- 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

8.2 In addition to this, Our Lady and St Joseph Catholic Primary School is committed to ensuring at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law (as explained in more detail in sections 14 and 16 below).

8.3 Our Lady and St Joseph Catholic Primary School is committed to complying with the principles in 8.1 at all times. This means that the School will:

- Inform individuals as to the purpose of collecting any information from them, as and when we ask for it;
- Be responsible for checking the quality and accuracy of the information;
- Regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the data retention policy;
- Ensure that when information is authorised for disposal it is done appropriately;
- Ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system, and follow the relevant security policy requirements at all times;
- Share personal information with others only when it is necessary and legally appropriate to do so;
- Set out clear procedures for responding to requests for access to personal information known as subject access requests;
- Report any breaches of the GDPR in accordance with the procedure in paragraph 9 below.

9. Legal Basis for Processing

9.1 The School will ensure that when processing data, it does so under one of the following available legal bases:-

- The individual has given consent that is specific to the particular type of processing activity, and that consent is informed, unambiguous and freely given.
- The processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps with regards to entering into a contract with the individual, at their request.
- The processing is necessary for the performance of a legal obligation to which we are subject.
- The processing is necessary to protect the vital interests of the individual or another.
- The processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in us as a school.

10. Use of Personal Data by Our Lady and St Joseph Catholic Primary School

10.1 Our Lady and St Joseph Catholic Primary School holds personal data on pupils, staff and other individuals such as visitors. In each case, the personal data must be treated in accordance with the data protection principles as outlined in paragraph 8.1 above.

Pupils

10.2 The personal data held regarding pupils includes contact details, assessment / examination results, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information, and photographs.

10.3 The data is used in order to support the education of the pupils, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well as a whole is doing, together with any other uses normally associated with this provision in a school environment.

10.4 May make use of limited personal data (such as contact details) relating to pupils, and their parents or guardians for fundraising, marketing or promotional purposes and to maintain relationships with pupils of the School, but only where consent has been provided to this.

10.5 In particular, Our Lady and St Joseph Catholic Primary School may:

- Transfer information to any association society or club set up for the purpose of maintaining contact with pupils or for fundraising, marketing or promotional purposes relating to but only where consent has been obtained first.
- Make personal data, including sensitive personal data, available to staff for planning curricular or extra-curricular activities;
- Use photographs of pupils in accordance with the photograph policy.
- Any wish to limit or object to any use of personal data should be notified to the Data Protection Officer (DPO) in writing, which will be acknowledged by in writing. If, in the view of the DPO the objection cannot be maintained, the individual will be given written reasons why the school can not comply with their request.

Staff

10.6 The personal data held about staff will include contact details, employment history, information relating to career progression, information relating to DBS checks, photographs.

10.7 The data is used to comply with legal obligations placed on in relation to employment, and the education of children in a school environment. may pass information to other regulatory authorities where appropriate, and may use names and photographs of staff in publicity and promotional material. Personal data will also be used when giving references.

10.8 Staff should note that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as "spent" once the period of the sanction has expired, the details of the incident may need to be kept for a longer period.

10.9 Any wish to limit or object to the uses to which personal data is to be put should be notified to the DPO who will ensure that this is recorded, and adhered to if appropriate. If the DPO is of the view that it is not appropriate to limit the use of personal data in the way specified, the individual will be given written reasons why cannot comply with their request.

Other Individuals

10.10 Our Lady and St Joseph Catholic Primary School may hold personal information in relation to other individuals who have contact with the school, such as volunteers and visitors. Such information shall be held only in accordance with the data protection principles, and shall not be kept longer than necessary.

11. Security of Personal Data

11.1 Our Lady and St Joseph Catholic Primary School will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this and their duties at Induction.

11.2 Our Lady and St Joseph Catholic Primary School will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

12. Disclosure of Personal Data to Third Parties

12.1 The following list includes the most usual reasons that the School will authorise disclosure of personal data to a third party:

- To give a confidential reference relating to a current or former employee, volunteer or pupil;
- For the prevention or detection of crime;
- For the assessment of any tax or duty;
- Where it is necessary to exercise a right or obligation conferred or imposed by law upon (other than an obligation imposed by contract);
- For the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);
- For the purpose of obtaining legal advice;
- For research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);
- To publish the results of public examinations or other achievements of pupils of;
- To disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips;
- To provide information to another educational establishment to which a pupil is transferring;
- To provide information to the Examination Authority as part of the examination process;
- To provide information to the relevant Government Department concerned with national education. At the time of the writing of this Policy, the Government Department concerned with national education is the Department for Education (DfE).The Examination Authority may also pass information to the DfE.

12.2 The DfE uses information about pupils for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual pupils cannot be identified from them. On occasion the DfE may share the personal data with other Government Departments or agencies strictly for statistical or research purposes.

12.3 Our Lady and St Joseph Catholic Primary School may receive requests from third parties (i.e. those other than the data subject, (or their representative) to disclose personal data it holds about pupils, their parents or guardians, staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation, which allow disclosure applies; or where necessary for the legitimate interests of the individual concerned.

12.4 All requests for the disclosure of personal data must be sent to the DPO who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

13 Confidentiality of Pupil Concerns

13.1 Where a pupil seeks to raise concerns confidentially with a member of staff and expressly with holds their agreement to their personal data being disclosed to their parents or guardian,

will maintain confidentiality unless it has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding their consent, or where believes disclosure will be in the best interests of the pupil or other pupils.

14 Subject Access Requests

14.1 Anybody who makes a request to see any personal information held about them by is making a subject access request. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure provided that they constitute a "filing system".

14.2 All requests should be sent to the DPO within 3 working days of receipt, and must be dealt with in full without delay and at the latest within one month of receipt.

14.3 Where a child or young person does not have sufficient understanding to make his or her own request (usually those under the age of 13, or over 13 but with a special educational need which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. The DPO must however, be satisfied that:

- The child or young person lacks sufficient understanding; and
- The request made on behalf of the child or young person is in their interests.

14.4 Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances must have written evidence that the individual has authorised the person to make the application and the DPO must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

14.5 Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

14.6 An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

14.7 All files must be reviewed by the DPO before any disclosure takes place. Access will not be granted before this review has taken place.

14.8 Where all the data in a document cannot be disclosed, a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

15 Exemptions to Access by Data Subjects or their Representative

15.1 Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived.

15.2 There are other exemptions from the right of subject access. If we intend to apply any of them to a request then we will usually explain which exemption is being applied and why.

16 Other Rights of Indivduals

16.1 Our Lady and St Joseph Chas an obligation to comply with the rights of individuals under the law, and takes these rights seriously. The following section sets out how will comply with the rights to:
- Object to Processing;
- Rectification;
- Erasure; and
- Data Portability.

16.2 Right to Object to Processing

16.2.1 An individual has the right to object to the processing of their personal data on the grounds of pursuit of a public interest or legitimate interest (grounds 4.5 and 4.6 above) where they do not believe that those grounds are made out.

16.2.2 Where such an objection is made, it must be sent to the DPO within 2 working days of receipt, and the DPO will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

16.2.3 The DPO shall be responsible for notifying the individual of the outcome of their assessment within fourteen working days of receipt of the objection.

16.3 Right to Rectification

16.3.1 An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, it should be sent to the DPO within 2 working days of receipt, and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified.

16.3.2 Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data, and communicated to the individual. The individual shall be given the option of, a review under the data protection complaints procedure, or an appeal direct to the Information Commissioner.

16.3.3 An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

16.4 Right to Erasure

16.4.1 Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:
- Where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;
- Where consent is withdrawn and there is no other legal basis for the processing;

- Where an objection has been raised under the right to object, and found to be legitimate;
- Where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);
- Where there is a legal obligation on to delete.

16.4.2 The DPO will make a decision regarding any application for erasure of personal data, and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other data controllers, and / or has been made public, reasonable attempts to inform those controllers of the request shall be made.

16.5 Right to Restrict Processing

16.5.1 In the following circumstances, processing of an individual's personal data may be restricted:
- Where the accuracy of data has been contested, during the period when is attempting to verify the accuracy of the data;
- Where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;
- Where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim;
- Where there has been an objection made under para 8.2 above, pending the outcome of any decision.

16.6 Right to Portability

16.6.1 If an individual wants to send their personal data to another organisation they have a right to request that provides their information in a structured, commonly used, and machine readable format. As this right is limited to situations where is processing the information on the basis of consent or performance of a contract, the situations in which this right can be exercised will be quite limited. If a request for this is made, it should be forwarded to the DPO within 2 working days of receipt, and the DPO will review and revert as necessary.

17 DATA BREACHES

17.1 GDPR aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

17.2 GDPR places obligations on staff to report actual or suspected data breaches and Our Lady and St Joseph Catholic Primary School's procedure for dealing with breaches is set out below.

17.3 Third Parties who process data on behalf of Our Lady and St Joseph Catholic Primary School will be required to notify the School of any data breach immediately they become aware of one.

17.4 Failure to notify the relevant individuals of a breach or suspected breach in line with this policy may be considered a disciplinary offence and appropriate action will be taken.

18. Responsible Parties

18.1 The School Data Protection Officer (DPO) has overall responsibility for breach notification within the School. They are responsible for ensuring breach notification processes are adhered to by all staff and are the designated point of contact for personal data breaches.

18.2 Mrs L Henderson is the first point of contact at Our Lady and St Joseph Catholic Primary School in the event of a suspected breach within the school.

19 **Procedure**

19.1 A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

19.1.1 Examples of a data breach could include the following (but are not exhaustive): -

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss);
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error (for example sending an email or SMS to the wrong recipient);
- Unforeseen circumstances such as a fire or flood;
- Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it.

19.2 The School must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

19.2.1 Examples of where the breach may have a significant effect includes: -

- Potential or actual discrimination;
- Potential or actual financial loss;
- Potential or actual loss of confidentiality;
- Risk to physical safety or reputation;
- Exposure to identity theft (for example through the release of non-public identifiers such as passport details);
- The exposure of the private aspect of a person's life becoming known by others.

19.2.2 If the breach is likely to result in a high risk to the rights and freedoms of individuals then the individuals must also be notified directly.

19.3 If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should contact the named contact for the school identified in **18.2**

19.4 Breach reporting is encouraged throughout the School and staff are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals.

19.5 Once reported, you should not take any further action in relation to the breach. In particular you must not notify any affected individuals or regulators or investigate further.

19.6 On being notified of a suspected personal data breach, the named contact for the school identified in 18.2 will notify the DPO. They will take immediate steps to establish whether a personal data breach has in fact occurred. If so they will take steps to:-

- Where possible, contain the data breach;
- As far as possible, recover, rectify or delete the data that has been lost, damaged or disclosed;
- Assess and record the breach in the School's data breach register;
- Notify the ICO;
- Notify data subjects affected by the breach;
- Notify other appropriate parties to the breach;
- Take steps to prevent future breaches.

19.7 The DPO will notify the ICO when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals. This will be done without undue delay and, where possible, within 72 hours of becoming aware of the breach. If the School are unsure of whether to report a breach, the assumption will be to report it.

19.8 Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO.

19.9 Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the DPO will notify the affected individuals without undue delay including the name and contact details of the ICO, the likely consequences of the data breach and the measures the School have (or intended) to take to address the breach.

19.10 When determining whether it is necessary to notify individuals directly of the breach, the named contact for the school identified in 18.2 will work with the DPO, the ICO and any other relevant authorities (such as the police).

19.11 If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the School will consider alternative means to make those affected aware (for example by making a statement on the School website).

20. Notifying Other Authorities

20.1 The School will need to consider whether other parties need to be notified of the breach. For example: -

- Insurers;
- Parents;
- Third parties (for example when they are also affected by the breach);
- Local authority;
- The police (for example if the breach involved theft of equipment or data). This list is non-exhaustive.

21. Assessing the Breach

21.1 Once initial reporting procedures have been carried out, the School will carry out all necessary investigations into the breach.

21.2 The School will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. We will identify ways to recover correct or delete data (for example notifying our insurers or the police if the breach involves stolen hardware or data).

21.3 Having dealt with containing the breach, the School will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include:

- What type of data is involved and how sensitive it is;
- The volume of data affected;
- Who is affected by the breach (i.e. the categories and number of people involved);
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise;
- Are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation);
- What has happened to the data;
- What could the data tell a third party about the data subject;
- What are the likely consequences of the personal data breach on the school; and
- Any other wider consequences which may be applicable.

22. Preventing Future Breaches

22.1 Once the data breach has been dealt with, the School will consider its security processes with the aim of preventing further breaches. In order to do this, we will: -

- Establish what security measures were in place when the breach occurred;
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again;
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice;
- Consider whether it is necessary to conduct a privacy or data protection impact assessment;
- Consider whether further audits or data protection steps need to be taken;
- To update the data breach register;
- To debrief governors/management following the investigation.

23. Reporting Data Protection Concerns

23.1 If an individual has a concern in relation to the way data is processed within the school or by a third party the school has a contract with, it is important that these concerns are raised with the named contact for the school identified in 18.2

24. Records Management

24.1 Records management is the process by which the Our Lady and St Joseph Catholic Primary School manages the 'records' held, whether in electronic format or paper

25. Retention Periods

25.1 In line with Article 5(1)(e) of the GDPR Our Lady and St Joseph Catholic Primary School will not retain personal data in an identifiable form for any longer than necessary. In determining an appropriate retention period for records containing personal data and those that do not,

Our Lady & St Joseph Catholic Primary School will take into account any applicable statutory limitation periods and any relevant guidance documents.

25.2 The School will undertake an Annual review of electronic and paper records to ensure they are retained in line with the School Retention Document.

26 Default Periods

26.1 The default period is the minimum period for which Our Lady and St Joseph Catholic Primary School will retain records. At the conclusion of the default period Our Lady and St Joseph Catholic Primary School will review the record being held and determine whether it can be destroyed.

26.2 The standard default period for retaining records will be as set out in the School Retention Document and will be recorded on the School Information Asset Register.

26.3 Our Lady and St Joseph Catholic Primary School will take into account the matters set out in Section 26 below in determining whether records will be retained beyond the default period.

27 Exceptions to the Default Period

27.1 In the majority of cases records will be securely disposed of when it reaches the end of the retention period. When assessing whether Data should be retained beyond the retention period Our Lady & St Joseph Catholic Primary School will consider whether:

- The record is subject to a current request pursuant to the GDPR.
- Our Lady and St Joseph Catholic Primary School is the subject of, or involved in ongoing legal action to which the record is or may be relevant.
- The record is or could be needed in connection with an ongoing investigation.
- The records are processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, and Our Lady & St Joseph Catholic Primary School has put in place appropriate technical and organisational measures.
- There are changes to the regulatory or statutory framework which require the records to be retained for a longer period.
- The data subject has exercised their right to restrict the processing of the their personal data contained in the records in accordance with Article 18 of the GDPR.

28 Disposal of Data

28.1 When records identified for disposal are destroyed, a register of the records destroyed will be kept (see Appendices).The destruction of records is an irreversible act and must be clearly documented. All records identified for disposal will be destroyed under confidential conditions by Our Lady and St Joseph Catholic Primary School.

28.2 Our Lady and St Joseph Catholic Primary School may sub-contract to another organisation its obligations to dispose of records under confidential conditions. The school satisfy itself of the sub- contractor/third party's experience and competence to do so.

29. Manual Records

29.1 Where records are held in paper or other manual form, the default period for retaining the record has expired and none of the exceptions for retaining records beyond the default period

at set out at Section 26 are satisfied, Our Lady and St Joseph Catholic Primary School will ensure the records are shredded or otherwise confidentially disposed of by Our Lady and St Joseph Catholic Primary School or by a person duly authorised by Our Lady and St Joseph Catholic Primary School to confidentially destroy the record.

30 Electronic Records

30.1 Where records are held in an electronic format Our Lady & St Joseph Catholic Primary School will where feasible use its reasonable endeavours to:

- Put the records beyond use so that the records are no longer on a live electronic system and cannot be accessed.
- Permanently delete the records from Our Lady and St Joseph Catholic Primary School electronic systems when and where this becomes possible Our Lady and St Joseph Catholic Primary School will only engage Data Processors that are able to provide sufficient guarantees in relation to secure disposal.

31. Freedom of Information

31.1 Our Lady and St Joseph Catholic Primary School is subject to the Freedom of Information Act 2000 (FOI) as a public authority, and as such, must comply with any requests for information in accordance with the principles laid out in the Act.

31.2 Any request for any information from Our Lady and St Joseph Catholic Primary School is technically a request under the FOI, whether or not the individual making the request mentions the FOI. Examples of requests are:-

- Copies of non confidential Minutes
- Statistical data
- Financial/ Budget data
- Staffing data
- Contract data

31.3 In all non-routine cases, if the request is simple and the information is to be released, then the individual who received the request can release the information, but must ensure that this is done within the timescale set out below. A copy of the request and response should then be sent to the DPO (Data Protection Officer).

31.4 All other requests should be referred in the first instance to the DPO], who may allocate another individual to deal with the request. This must be done promptly, and in any event within 3 working days of receiving the request.

31.5 When considering a request under FOI, you must bear in mind that release under FOI is treated as release to the general public, and so once it has been released to an individual, anyone can then access it, and you cannot restrict access when releasing by marking the information “confidential” or “restricted”.

32 Time Limit for Compliance

32.1 Our Lady and St Joseph Catholic Primary School must respond as soon as possible, and in any event, within 20 working days of the date of receipt of the request. When calculating the 20 working day deadline, a “working day” is a school day (one in which pupils are in attendance), subject to an absolute maximum of 60 normal working days (not school days) to respond.

33 Procedure for dealing with a request

33.1 When a request is received that cannot be dealt with by simply providing the information, it should be referred in the first instance to the DPO who may re-allocate to an individual with responsibility for the type of information requested.

33.2 The first stage in responding is to determine whether or not Our Lady and St Joseph Catholic Primary School "holds" the information requested. Our Lady and St Joseph Primary School will hold the information if it exists in computer or paper format. Whilst the School is not obliged to create new information, it will be expected to create reports or extract data from existing systems, unless that process exceeds the appropriate limits for complying with a request.

33.3 The second stage is to decide whether the information can be released, or whether one of the exemptions set out in the Act applies to the information. Common exemptions that might apply include:

- Section 40 (1) – the request is for the applicants personal data. This must be dealt with under the subject access regime in the DPA, detailed in paragraph 9 of the DPA policy above;
- Section 40 (2) – compliance with the request would involve releasing third party personal data, and this would be in breach of the DPA principles as set out in paragraph 3.1 of the DPA policy above;
- Section 41 – information that has been sent to (but not own information) which is confidential;
- Section 21 – information that is already publicly available, even if payment of a fee is required to access that information;
- Section 22 – information that intends to publish at a future date;
- Section 43 – information that would prejudice the commercial interests of and / or a third party;
- Section 38 – information that could prejudice the physical health, mental health or safety of an individual (this may apply particularly to safeguarding information);
- Section 31 – information which may prejudice the effective detection and prevention of crime – such as the location of CCTV cameras;
- Section 36 – information which, in the opinion of the chair of governors of , would prejudice the effective conduct of . There is a special form for this on the ICO's website to assist with the obtaining of the chair's opinion.

33.4 Sections 22, 43, 31 and 36 are qualified exemptions. This means that even if the exemption applies to the information, you also have to carry out a public interest weighting exercise, balancing the public interest in the information being released, as against the public interest in withholding the information.

34 Responding to a request

35.1 When responding to a request where Our Lady and St Joseph Catholic Primary School has withheld some or all of the information, you must explain why the information has been withheld, quoting the appropriate section number and explaining how the information

requested fits within that exemption. If the public interest test has been applied, this also needs to be explained.

35.2 The letter should end by explaining to the requestor how they can complain – either by reference to an internal review by a governor, or by writing to the ICO. An Internal Review should be a thorough reconsideration of the request in the context of the requester's appeal. The conclusion of the review may result in the disclosure of information initially defined as exempt. The School should aim to complete an internal review within 20 working days, up to a maximum of 40 working days.

The School's Data Protection Officer is

School DPO: Mrs Henderson
Our Lady & St Joseph Catholic Primary School
Wades Place
E14 0DE
office@olsj.co.uk
0203 764 8860

External Consultant DPO:
Naomi Korn Associates Ltd.,
Connetix IT & Consultancy
IG@Connetix.co.uk

1. Child Protection **These retention periods should be used in conjunction with the OLSJ policy "Safeguarding Children and Safer Recruitment in Education" Latest Version**						
	Basic File Description	**Data Protection Issues?**	**Statutory Provisions**	**Retention Period**	**Action at end of the administrative life of the record**	
1.1	Child Protection Files	YES	Education Act 2002, s175, related guidance "Safeguarding Children in Education", September 2004	DOB + 25 years [1]	SHRED – SECURE DISPOSAL	
1.2	Allegation of a child protection nature against a member of staff, including where the allegation is unfounded	YES	Employment Practices Code: Supplementary Guidance 2.13.1 (Records of Disciplinary and Grievance) Education Act 2002 guidance "Dealing with Allegations of Abuse against Teachers and Other Staff" November 2005	Until person's normal retirement age, or 10 years from the date of allegation, whichever is longer	SHRED – SECURE DISPOSAL	

2. Governors						
2.1	Minutes • Principal Set • Inspection Copies	NO NO		Permanent Date of meeting + 3years	Retain in school for 6 years from date of meeting, then transfer to archives SHRED – SECURE DISPOSAL	
2.2	Agendas	NO		Date of Meeting	SHRED – SECURE DISPOSAL	
2.3	Reports	NO		Date of report + 6years	Retain in school for 6 years from date of meeting	
2.4	Annual Parents meeting papers	NO		Date of meeting + 6years	Retain in school for 6years from date of meeting.	
2.5	Instruments of Government	NO		Permanent	Retain in school whilst school is open.	
2.6	Trusts and Endowments	NO		Permanent	Retain in school whilst operationally required	
2.7	Action Plans	NO		Date of action plan +3years	SHRED – SECURE DISPOSAL	
2.8	Policy Documents	NO		Expiry of Policy	Retain in school whilst policy is operational (this includes if the expired policy is part of a past decision making process)	
2.9	Complaints files	YES		Date of resolution of complaint +6years	Retain in school for the first 6 years. Review for further retention in the case of contentious disputes SHRED routine complaints	

2.10	Annual Reports required by the Department for Education and Skills	NO		Date of report +10years[1]		
2.11	Proposals for schools to become, or ne established as Specialist Status schools	NO		Current year +3years	SHRED – SECURE DISPOSAL	

3. Management						
3.1	Log Books	YES[2]		Date of last entry in book +6years	SHRED - – SECURE DISPOSAL	
3.2	Minutes of Senior Management Team and other internal administrative bodies meetings	YES[1]		Date of meeting +7years	SHRED – SECURE DISPOSAL.	
3.3	Reports made by the head teacher or the management team	YES[1]		Date of report +3years	SHRED – SECURE DISPOSAL	
3.4	Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	YES[1]		Closure of file + 6years	SHRED – SECURE DISPOSAL	
3.5	Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	NO		Date of correspondence + 3years	SHRED – SECURE DISPOSAL	
3.6	Professional Development Plans	YES		Closure + 6years	SHRED – SECURE DISPOSAL	
3.7	School Development Plans	NO		Closure + 6years	Review	
3.8	Admissions- if admission is successful	YES		Admission + 1Year	SHRED – SECURE DISPOSAL	
3.9	Admissions – if appeal unsuccessful	YES		Resolution of case + 1year	SHRED – SECURE DISPOSAL	

3.10	Admissions – Secondary Schools- Casual	YES		Current year + 1year	SHRED – SECURE DISPOSAL	
3.11	Proof of address supplied by parents as part of admissions process	YES		Current year + 1year	SHRED – SECURE DISPOSAL	

4. Pupils						
4.1	Admission Register	YES		Date of last entry in the book + 6years	Retain in school for 6 years from date of last entry, transfer to archives	
4.2	Attendance Registers	YES		Date of Register + 3years	SHRED/ If these records are retained electronically any back up copies should be destroyed at the same time	
4.3a	Pupil Record Cards • Primary	YES		Retain for the time which the pupil remains at the primary school	Transfer to secondary or other primary school when child leaves. In case of exclusion it may be appropriate to transfer the record to the Behaviour Service	
4.3b	• Secondary		Limitation Act 1980	DOB of pupil + 25years[3]	SHRED – SECURE DISPOSAL	
4.4a	Pupil Record Cards • Primary	YES		Retain for the time which the pupil remains at the primary school	Transfer to secondary or other primary school when child leaves. In case of exclusion it may be appropriate to transfer the record to the Behaviour Service	
4.4b	• Secondary		Limitation Act 1980	DOB of pupil + 25years[4]	SHRED – SECURE DISPOSAL	

4.5	Special Education Needs files, reviews and Individual Education Plans	YES		DOB of the pupil + 25 years the review NOTE: This retention period is the minimum period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period.	SHRED – SECURE DISPOSAL	
4.6	Letters authorising absence	NO		Date of absence +2years	SHRED – SECURE DISPOSAL	
4.7	Absence Book	NO		Current year + 6years	SHRED – SECURE DISPOSAL	
4.8a 4.8b	Examination Results • Public • Internal examination results	YES NO YES		Year of examinations + 6years Current year + 5years[5]	SHRED – SECURE DISPOSAL SHRED – SECURE DISPOSAL	
4.9	Any other records created in the course of contact with pupils	YES/ NO		Current year +3years	Review at the end of 3 years and either allocate a further retention period or SHRED – SECURE DISPOSAL	
4.10	Statement mained under The Education Act 1996 – section 324	YES	Special Education Needs and Disability Act 2001 Section 1	DOB + 30years	SHRED – SECURE DISPOSAL unless legal action is pending	

4.11	Proposed statement or amended statement	YES	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30years	SHRED - SECURE DISPOSAL unless legal action is pending	
4.12	Advice and information to parents regarding educational needs	YES	Special Educational Needs and Disability Act 2001 Section 2	Closure + 12years	SHRED – SECURE DISPOSAL unless legal action is pending	
4.13	Accessibility Strategy	YES	Special Educational Needs and Disability Act 2001 Section 14	Closure + 12years	SHRED – SECURE DISPOSAL unless legal action is pending	
4.14	Children's SEN Files	YES		DOB of pupil + 25years then review – it may be appropriate to add an additional retention period in certain cases	SHRED – SECURE DISPOSAL unless legal action is pending	
4.15	Parental permission slips for school trips – where there has been no major incident	YES		Conclusion of trip	SHRED – SECURE DISPOSAL	
4.16	Parent permission slip for school trips – where there has been a major incident	YES	Limitation Act 1980	DOB of the pupils involved in incident + 25years The permission slips for all pupils on the trip need to be retained to show that the rules had been followed for all pupils	SHRED – SECURE DISPOSAL	
4.17	Records created by school to obtain approval to run an Educational Visit outside the classroom – Primary Schools	NO	3 part supplement to the Health & Safety of Pupils on Educational Visits (HASPEV) 1998	Date of visit + 14years[6]	SHRED or DELETE securely	
4.18	Records created by school to obtain approval to run an Educational Visit outside the	NO	3 part supplement to the Health & Safety of Pupils on Educational Visits (HASPEV) 1998	Date of visit + 10 years[7]	SHRED or DELETE securely	

	classroom – Secondary Schools					

5. Curriculum						
5.1	Curriculum development	NO		Current Year + 6years	SHRED – SECURE DISPOSAL	
5.2	Curriculum returns	NO		Current Year + 3years	SHRED – SECURE DISPOSAL	
5.3	School syllabus	NO		Current Year +1year	It may be appropriate to review these records at the end if each year and allocate a new retention period or SHRED – SECURE DISPOSAL	
5.4	Schemes of work	NO		Current Year +1year	It may be appropriate to review these records at the end if each year and allocate a new retention period or SHRED – SECURE DISPOSAL	
5.5	Timetable	NO		Current Year +1year	It may be appropriate to review these records at the end if each year and allocate a new retention period or SHRED – SECURE DISPOSAL	
5.6	Class Record Books	NO		Current Year +1year	It may be appropriate to review these records at the end if each year and allocate a new retention period or SHRED – SECURE DISPOSAL	
5.7	Mark Books	NO		Current Year +1year	It may be appropriate to review these records at the end if each year and allocate a new retention period or SHRED – SECURE DISPOSAL	

5.8	Record of Homework Set	NO		Current Year +1year	It may be appropriate to review these records at the end if each year and allocate a new retention period or SHRED – SECURE DISPOSAL	
5.9	Pupils' Work	NO		Current Year +1year	It may be appropriate to review these records at the end if each year and allocate a new retention period or SHRED – SECURE DISPOSALS	
5.10	Examination Results	YES		Current Year + 6years	SHRED – SECURE DISPOSAL	
5.11	SATS Records	YES		Current Year + 6years	SHRED – SECURE DISOSAL	
5.12	PAN Records	YES		Current Year + 6years	SHRED – SECURE DISPOSAL	
5.13	Value added records	YES		Current Year +6years	SHRED – SECURE DISPOSAL	

6. Personnel Records held in Schools						
6.1	Timesheets, sick pay	YES	Financial Regulations	Current Year +6years	SHRED – SECURE DISPOSAL	
6.2	Staff Personal Files	YES		Termination +7years	SHRED – SECURE DISPOSAL	
6.3	Interview notes and recruitment records	YES		Date of Interview + 6months	SHRED – SECURE DISPOSAL	
6.4	Pre-employment vetting information (inc CRB checks)	NO	CRB Guidelines	Date of check + 6moths	SHRED – SECURE DISPOSAL - by designated member of staff	
6.5	Disciplinary Proceedings:	YES	**WHERE THE WARNING RELATES TO CHILD PROTECTION ISSUES SEE 1.2. If the disciplinary proceedings relate to a child protection matter please contact your safeguarding children officer for further advice.**			
6.5a	• Oral Warning			Date of Warning + 6months	SHRED – SECURE DISPOSAL	
6.5b	• Written Warning – level 1			Date of Warning + 6months	SHRED – SECURE DISPOSAL	
6.5c	• Written Warning – level 2			Date of warning +12months	SHRED – SECURE DISPOSAL	
6.5d	• Final Warning			Date of Warning +18months	SHRED – SECURE DISPOSAL	
6.5e	• Case not found			If child protection related please see 1.2 otherwise shred immediately at the conclusion of the case	SHRED – SECURE DISPOSAL	
6.6	Records relating to accident/injury at work	YES		Date of incident +12years. In the case of serious accidents a further retention period will need to be applied	SHRED – SECURE DISPOSAL	
6.7	Annual appraisal/assessment records	NO		Current year +5years	SHRED – SECURE DISPOSAL	
6.8	Salary Cards	YES		Last date of employment +85years	SHRED – SECURE DISPOSAL	
6.9	Maternity pay records	YES	Statutory Maternity Pay (General)	Current year +3years	SHRED – SECURE DISPOSAL	

			Regulations 1986 (SI 1986/1960), revised 1999 (SI 1999/567)			
6.10	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	YES		Current year +6years	SHRED – SECURE DISPOSAL	
6.11	Proofs of identity collected as part of the process of checking “portable” enhanced CRB disclosure	YES		Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff’s personal file		

7. Health & Safety						
7.1	Accessibility		Disability Discrimination Act	Current year +6years	SHRED – SECURE DISPOSAL	
7.2	Accident Reporting		Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980			
7.2a	• Adults	YES		Date of Incident +7years	SHRED – SECURE DISPOSAL	
7.2b	• Children	YES		DOB of child +25years[8]	SHRED – SECURE DISPOSAL	
7.3	COSHH			Current year +10 years (where appropriate an additional retention period may be allocated)		
7.4	Incident Reports	YES		Current year +20years	SHRED – SECURE DISPOSAL	
7.5	Policy Statements			Date of Expiry +1year	SHRED – SECURE DISPOSAL	
7.6	Risk Assessments			Current Year +3years	SHRED – SECURE DISPOSAL	
7.7	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos			Last action + 40years	SHRED – SECURE DISPOSAL	
7.8	Process of monitoring of areas			Last action +50years	SHRED – SECURE DISPOSAL	

	where employees and persons are likely to have come in contact with radiation					
7.9	Fire Precautions log book			Current year +6years	SHRED – SECURE DISPOSAL	

8. Administrative						
8.1	Employers Liability Certificate			Closure of the school +40years	SHRED – SECURE DISPOSAL	
8.2	Inventories of Equipment & Furniture			Current year +6years	SHRED – SECURE DISPOSAL	
8.3	General File Series			Current year +5years	Review to see whether a further retention period is required.	
8.4	School brochure or prospectus			Current year +3years		
8.5	Circulars (staff/pupils/parent)			Current year +1year	SHRED – SECURE DISPOSAL	
8.6	Emails			1 Year	Delete after 1 school term. Permanent Deletion after 1 school year.	
8.7	Newsletters, ephemera			Current year +1year	Review to see whether a further retention period is required.	
8.8	Visitors Book			Current year +2years	Review to see whether a further retention period is required.	
8.9	PTA/Old pupils Association			Current year +6years	Review to see whether a further retention period is required.	

9. Finance						
9.1	Annual Accounts		Financial Regulations	Current year +6years		
9.2	Loans and Grants		Financial Regulations	Date of last payment on loan +12years	Review to see whether a further retention period is required.	
9.3 9.3a 9.3b 9.3c	Contracts • Under Seal • Under Signature • Monitoring Records			 Contract Completion date +12years Contract Completion date +6years Current year +2 years	 SHRED – SECURE DISPOSAL SHRED – SECURE DISPOSAL SHRED – SECURE DISPOSAL	
9.4	Copy Orders			Current year +2years	SHRED – SECURE DISPOSAL	
9.5	Budgeting reports, budget monitoring etc			Current year +3years	SHRED – SECURE DISPOSAL	
9.6	Invoice, receipts and other records covered by the Financial Regulations		Financial Regulations	Current year +6years	SHRED – SECURE DISPOSAL	
9.7	Annual Budget and background papers			Current year +6years	SHRED – SECURE DISPOSAL	
9.8	Order Books and Requisitions			Current year +6years	SHRED – SECURE DISPOSAL	
9.9	Delivery Documentation			Current year +6years	SHRED – SECURE DISPOSAL	
9.10	Debtors' Records		Limination Act 1980	Current year +6years	SHRED – SECURE DISPOSAL	
9.11	School Fund – Cheque Book			Current year +3years	SHRED – SECURE DISPOSAL	
9.12	School Fund – Paying in Books			Current year +6years then review	SHRED – SECURE DISPOSAL	
9.13	School Fund – Ledger			Current year +6years then review	SHRED – SECURE DISPOSAL	
9.14	School Fund – Invoices			Current year +6years then review	SHRED – SECURE DISPOSAL	
9.15	School Fund – Receipts			Current year +6years then review	SHRED – SECURE DISPOSAL	
9.16	School Fund – Bank Statements			Current year +6years then review	SHRED – SECURE DISPOSAL	

9.17	School Fund - School Journey Books			Current year +6years then review	SHRED – SECURE DISPOSAL	
9.18	Applications for free school meals, travel, uniforms etc			Whilst child at school	SHRED – SECURE DISPOSAL	
9.19	Student grant applications			Current year +3years	SHRED – SECURE DISPOSAL	
9.20	Free school meals registers	YES	Financial Regulations	Current year +6years	SHRED – SECURE DISPOSAL	
9.21	Petty Cash Books		Financial Regulations	Current year +6years	SHRED – SECURE DISPOSAL	

10. Property						
10.1	Title Deeds			Permanent	Permanent, these should follow the property unless property has been registered at the Land Registry. Offer to archives if deeds no longer needed.	
10.2	Plans			Permanent	Retain in school whilst operational. Offer to archives[9]	
10.3	Maintenance and Contractors		Financial Regulations	Current year +6years	SHRED – SECURE DISPOSAL	
10.4	Leases			Expiry of lease +6years	SHRED – SECURE DISPOSAL	
10.5	Lettings			Current Year +3years	SHRED – SECURE DISPOSAL	
10.6	Burglary, theft and vandalism report forms			Current year +6years	SHRED – SECURE DISPOSAL	
10.7	Maintenance log books			Last entry +6 years	SHRED – SECURE DISPOSAL	
10.8	Contractors' Reports			Current year +6years	SHRED – SECURE DISPOSAL	

11. Local Education Authority						
11.1	Secondary transfer sheets - Primary	YES		Current year +2years	SHRED – SECURE DISPOSAL	
11.2	Attendance Returns	YES		Current year +1year	SHRED – SECURE DISPOSAL	
11.3	Circular From LEA			Whilst required operationally	Review to see whether a further retention period is required.	

12. Department for children, Schools and Families						
12.1	HMI reports			These do not need to be kept any longer		
12.2	OFSTED reports and papers			Replace former report with any new inspection report	Review to see whether a further retention period is required.	
12.3	Returns			Current year +6years	SHRED – SECURE DISPOSAL	
12.4	Circulars from Department for Children, Schools and Families			Whilst operationally required	Review to see if further retention period is required.	

13. Connexions						
13.1	Service level agreement			Until Superseded	SHRED – SECURE DISPOSAL	
13.2	Work Experience agreement			DOB of child +18years	SHRED – SECURE DISPOSAL	

14. School Meals						
14.1	Dinner Register			Current +3years	SHRED – SECURE DISPOSAL	
14.2	School Meals Summary Sheets			Current +3years	SHRED – SECURE DISPOSAL	

15. Family Liaison Officers and Parent Support Assistants						
15.1	Day Books	YES		Current year +2years then review	SHRED – SECURE DISPOSAL	
15.2	Reports for outside agencies – where the report has been included on the case file created by the outside agency	YES		Whilst child is attending the school then destroy	SHRED – SECURE DISPOSAL	
15.3	Referral forms	YES		While the referral is current	SHRED – SECURE DISPOSAL	
15.4	Contact Data Sheets	YES		Current year then review, if contact is no longer active then destroy	SHRED – SECURE DISPOSAL	
15.5	Contact database entries	YES		Current year then review, if contact is no longer active then destroy	DELETE	
15.6	Group Register	YES		Current year +2years	SHRED – SECURE DISPOSAL	

16. Early Years Provision						
16.1. Records to be kept by Registered Persons – All Care						
16.1.1	The name, home address and date of birth of each child who is looked after on the premises	YES		Closure of setting + 50 years [These could be required to show whether or not an individual child attended the setting in a child protection investigation]	SHRED – SECURE DISPOSAL	
16.1.2	The name, home address and telephone number of a parent of each child who is looked after on the premises	YES		If this information is kept in the same book or on the same form as in 16.1.1 then the same retention period should be used as in 16.1.1 If the information is stored separately, then destroy once the child has left the setting (unless the information is collected for anything other than emergency contact)	SHRED – SECURE DISPOSAL	
16.1.3	The name, address and telephone number of any person who will be looking after children on the premises	YES		See 16.4.5 below		
16.1.4	A daily record of the names of children looked after on the premises, their hours of attendance and the names of the persons who looked after them		The Day Care and Child Minding (National Standards) (England) Regulations 2003	The regulations say that these records should be kept for 2 years (SI20031996 7(1b)). If these records are likely to be needed in a child protection setting (see 16.1.1 above) then the records should be		

				retained for closure of setting + 50 years		
16.1.5	A record of accidents occurring on the premises and incident books relating to other incidents	YES	The Day Care and Child Minding (National Standards) (England) Regulations 2003[10]	DOB of the child involved in the accident or the incident + 25 years If an adult is injured then the accident book must be kept for 7 years from the date of the incident		
16.1.6	A record of any medicinal product administered to any child on the premises, including the date and circumstances of its administration, by whom it was administered, including medicinal products which the child is permitted to administer to himself, together with a record of parent's consent	YES	The Day Care and Child Minding (National Standards) (England) Regulations 2003[11]	DOB of the child being given/taking the medicine + 25 years		
16.1.7	Records of transfer	YES		One copy is to be given to the parents, one copy transferred to the Primary School where the child is going		
16.1.8	Portfolio of work, observations and so on	YES		To be sent home with child		
16.1.9	Birth Certificate	YES		Once the setting has had sight of the birth certificate and recorded the necessary information the original can be returned to the parents. There is no requirement		

				to keep a copy of the birth certificate.		

16.2.	**Records to be kept by Registered Persons – All Care**					
16.2.1	The name and address and telephone number of the registered person and every other person living or employed on the premises	YES	The Day Care and Child Minding (National Standards) (England) Regulations 2003	See 16.4 below		
16.2.2	A statement of the procedure to be followed in the event of a fire or accident	NO		Procedure superseded +7years		
16.2.3	A statement of the procedure to be followed in the event of a child being lost or not collected	NO		Procedure superseded +7years		
16.2.4	A statement of the procedure to be followed where a parent has a complaint about the service being provided by the registered person	NO		Until Superseded		
16.2.5	A statement of the arrangements in place for the protection of children, including arrangements to safeguard the children from abuse or neglect and procedures to be followed in the event of allegations of abuse or neglect	NO		Closure of setting +50years (these could be required to show whether or not an individual child attended the setting in a child protection investigation)		
16.3 Records to be kept by Registered persons – Overnight provisions – Under 2's						

16.3.1	Emergency contact details for appropriate adult to collect the child if necessary	YES		Destroy once child has left the setting (unless the information collected for anything other than emergency contact)		
16.3.2	Contract, signed by the parent, stating all the relevant details regarding the child and their care, including the name of the emergency contact and confirmation of their agreement to collect the child during the night	YES		Date of birth of the child who is the subject of the contract +25years		
16.4 Other Records – Administration						
16.4.1	Financial Records – Accounts, statements, invoices, petty cash etc	NO		Current year +6years		
16.4.2	Insurance policies – Employers Liability	NO	Employers Liability Financial Regulations	The policies are kept for a minimum of 6 years and a maximum of 40 years depending on the type of policy		
16.4.3	Claims made against insurance policies – damage to property	YES		Case concluded +3years		
16.4.4	Claims made against insurance policies – personal injury	YES		Case concluded +6years		
16.4.5	Personal Files – Records relating to an individual's employment history	YES[12]		Termination +6years then review		

16.4.6	Pre-employment vetting information (including CRB checks)	NO	CRB guidelines	Date of check +6months		
16.4.7	Staff training records – general	YES		Current year +2years		
16.4.8	Training (proof of completion such as certificates, awards, exam results)	YES		Last action +7years		
16.4.9	Premises and Health & Safety • Premises Files (relating to maintenance) • Risk Assessment	NO		• Cessation of use of building +7years then review • Current year +3years		

[1]This amendment has been made in consultation with the Safeguarding Children Group
[2]From January 1st 2005 subject access is permitted into unstructured filling systems and log books and other records created within the school containing details about the activities of individual pupils and members of staff will become subject to the General Data Protection Regulation 2018
[3]In the case of exclusion it may be appropriate to transfer the record to the Behaviour Service
[4]As Above
[5]If these records are retained on the pupil file or in their National record of Achievement they need only be kept for as long as operationally necessary
[6]This retention period has been set in agreement with the Safeguarding Children's Officer
[7]If this is placed on a personal file it must be weeded from the file
[8]A child may make a claim for negligence for 7 years from their 18th Birthday. To ensure that all records are kept until the pupil reaches the age of 25 this retention period has been applied
[9]If the property has been sold private housing then the archives service will embargo these records for an appropriate period of time to prevent them being used to plan or carry out a crime

[10]The regulations say that these records should be kept for 2 years (SI20031996 7(1b)). The Statute of Limitations states that a minor may make a claim for 7 years from their 18th Birthday, therefore the retention should be for the longer period.
[11]The regulations say that these records should be kept for 2 years (SI200319967(1b)). The NHS records retention schedule states that nay records relating to a child under the age of 18 should be retained until that child reaches the age of 25 years. Therefore, the retention should be DOB of the child being given/taking the medicine +25years

[12]For General Data Protection Regulation purposes the following information should be kept on the file for the following periods:	
• All documentation on the personal file	Duration of employment
• Pre-employment & vetting information	Start date +6months
• Records relating to accident or injury at work	Minimum of 12 years
• Annual appraisal/assessment records	Minimum of 5 years
Records relating to disciplinary matters (kept on personal file)	
• Oral	6 months
• First level warning	6 months
• Second level warning	12 months
• Final Warning	18 months

File Name/No	Reason for Disposal	Date	Disposed By:

Source of information	Asset number or ID	Name of asset	Description	What is the information used for?	GDPR Legal Basis	Location	Owner	Volume	Personal data	Format	Access	Shared	Retention	Control measures	Key asset
STAFF (including , students, volunteers)	1	Staff employment files	Holds employment information, including name, home address and telephone number for each employee, student, volunteer, director. Training certificates and references, application forms. Confidential information relating to each employee, including ID information, right to work in the UK, health and medical needs, suitability declaration forms, sickness and leave details, return to work forms, individual risk assessments, employment terms and conditions and occupational health reports; Disciplinary Information	- To ensure the suitability of staff; - To ensure staff are contactable; - To evidence appropriate recruitment checks have been undertaken; - Evidence purpose of any alligations/dismissals - To ensure suitable actions were taken - To meet requirements of the school	- Consent - Contract - Legal Obligation - Public Task	Computer files held on cloud; Archived information stored in locked cupboard; Paper documents stored in secure, fixed filing cabinet on site.	SBM	64 current files; 41 archived files; Total 105	Yes; includes sensitive personal data	Paper files stored in secure locked filing cabinet; Password protected Integris system, and word documents.	Access is restricted to named senior managers and registered person.	Information is shared with senior managers, Ofsted and the local authority where required for safeguarding and child protection purposes.	Termination +7yrs	Restricted authorised only access to files; Secure, locked storage; Information kept on site at all times Password protected electronic files; Regular review and update of information for accuracy and relevance; Effective archiving and deletion procedures.	Yes
	2	Performance management files	Holds supervision and appraisal information; performance management records.	- To provide support - To help employees achieve their goals - Identify and provide necessary training - To meet school requirements	- Consent - Contract	Archived information stored in locked cupboard; Paper documents stored in secure, fixed filing cabinet on site.	Head	64 Current files; 41 archived files; Total 105	Yes; includes sensitive personal data	Paper files stored in secure locked cabinet	Access is restricted to SLT/SBM/Admin Staff	Information is shared with senior managers, Ofsted and the local authority where required for safeguarding and child protection purposes.	Current year +5yrs	Secure, locked storage; Information kept onsite at all times. Regular review and update of information for accuracy and relevance.	Yes
	3	DBS records	Includes details of spent/unspent convictions, cautions, reprimands and police issued final warnings; any additional information held by local police deemed relevant to the role and checks of the DBS barred lists.	- To ensure the suitability of staff; - To evidence appropriate recruitment checks have been undertaken; - To meet requirements of the school	- Consent - Contract - Legal Obligation - Public Task - Legitimate Interest	Paper Documents stored in secure, fixed filing cabinet onsite.	SBM	12 Current Files	Yes; includes sensitive personal data	Paper files stored in secure locked cabinet	Access is restricted to SLT/SBM/Admin Staff	Information is shared with senior managers, Ofsted and the local authority where required for safeguarding and child protection purposes.	6 Months	Secure, locked storage; Information kept onsite at all times. Regular review and update of information for accuracy and relevance.	Yes

	4	SLT meeting minutes	Minutes of staff meetings, including possible discussion about children.	- To identify/rectify issues - To provide staff support - To provide Student/Parent support - To meet school requirements	- Legal Obligation - Public Interest	Archived information stored in locked cupboard; Paper documents stored in secure, fixed filing cabinet on site; Password protected word/excel.	SLT	1 Current File **(2021/22)** 20 Archived Files **(2017/18) (2018/19) (2019/20) (2020/21)** Total **21**	Yes; possible to include sensitive personal data if child discussed	Original notes to be destroyed once copied electronically; Password protected word documents.	Access restricted to SLT	Information is shared with SLT, school staff; Ofsted and the local authority where required for safeguarding and child protection purposes.	Date of Meeting +7yr	Information kept on site at all times Password protected electronic files;	Yes; if child discussed
	5	Staff registers	Details of staff present including times of arrival and departure	-To identify staff on site incase of emergency - To meet school requirments	- Legal Obligation - Vital Interest	Password protected system Archived information stored in locked cupboard	SBM/Head/Admin		Yes;	Password protected system	Access restricted	Information is shared with SLT, Local authority; emergency services where required incase of emergency	6yrs	Information kept on site at all times Password protected electronic files;	Yes
	6	Payee information (Salary Cards)	Includes details of wages, NI and tax contributions; NI number, personnel number, tax code and bank details	- To ensure salary payment	- Consent - Contract - Legal Obligation	Archived information stored in locked cupboard; Paper documents stored in secure, fixed filing cabinet on site; Password protected system	SBM/Head/Local Authority	64 current files; 41 archived files; Total 105	Yes;	Password protected system	Access restricted SBM/SLT	Information is shared with Local Authority	Termination Date +85yrs	Restricted authorised only access to files; Secure, locked storage; Information kept on site at all times Password protected electronic files; Regular review and update of information for accuracy and relevance; Effective archiving and deletion procedures.	Yes

	7	Financial information	Incomings and outgoings, tax details, bank details, profits and loss, debts, business funding details. Also funding details for EYFS; Pupil Premium and Inclusion funding details.	- To meet school requirements	- Legal Obligation - Public Task - Legitimate Interest	Archived information stored in locked cupboard; Paper documents stored in secure, fixed filing cabinet on site; Password protected system	SBM/Head Governors/Local Authority when required	1 Current File **(2021/22)** 3 Archived Files **(2018/19) (2019/20) (2020/21)** Total 4	Yes	Password protected system	Access restricted SBM/Head/Finance Officer	Information is shared with senior managers, Ofsted and the local authority where required	6yrs	Restricted authorised only access to files; Secure, locked storage; Information kept on site at all times Password protected electronic files; Regular review and update of information for accuracy and relevance; Effective archiving and deletion procedures.	Yes
	8	Emergency contacts	Emergency contact details of staff, including next of kin.	- To meet school requirements - To provide staff support - Incase of emergency	- Consent - Contract - Legal Obligation - Vital Interest - Public Task - Legitimate Interest	Computer files held on cloud; Archived information stored in locked cupboard; Paper documents stored in secure, fixed filing cabinet on site.	SBM/Head	64 current files; 41 archived files; Total 105	Yes	Paper files stored in secure locked filing cabinet; Password protected system.	Access restricted SBM/Head/SLT	Information is shared with SLT, Local authority; emergency services where required incase of emergency	Termination +7yrs	Restricted authorised only access to files; Secure, locked storage; Information kept on site at all times Password protected electronic files; Regular review and update of information for accuracy and relevance; Effective archiving and deletion procedures.	Yes
CHILDREN/ PARENT	9	Application/Admissions Forms	Enrolment details, including name, home address, Birth Cert, Baptism Cert, Proof of Address, Religion, parents'/carers' details, confirmation of parental responsibility;	- To ensure child correctly ranked/placed in school - To meet Local Autority Requirments - To ensure Admissions Policy adhered to - To meet school requirements	- Consent - Contract - Public Task	Paper Documents stored in secure, fixed filing cabinet onsite. Archived information stored in locked cupboard	Admissions Officer/SBM/Admin	0 Current Files 0 Archived Files **Total** 0	Yes	Paper files stored in secure locked filing cabinet.	Access restricted Admissions Officer/SBM/Admin	Information shared with Local Authority and SENCO where required	**Successful Admission** - Admission Date +1yr **Unsuccessful Admission -** Resolution Date + 1yr	Secure, locked storage; Information kept onsite at all times. Regular review amd update of information for accuracy and relevance.	Yes

		Child Files	Application Details, Parent name and address; name, address, birth cert, baptism cert, proof of address, religion, tel no, parent/carer details, emergency contact details, ethnicity, first language etc; Medical and allergy information previous school details, school reports, parent consultations, any correspondance between school and parent;	- To ensure child correctly ranked/placed in school - To meet Local Autority Requirments - To ensure Admissions Policy adhered to - To meet school requirements - To provide help and support where needed	- Consent - Contract - Legal Obligation - Vital Interest - Public Task - Legitimate Interest	Computer files held on cloud; Archived information stored in locked cupboard; Paper documents stored in secure, fixed filing cabinet on site.	SLT/SBM/Admin	448 Current Files Total 448	Yes	Paper files stored in secure locked filing cabinet; Password protected Integris system, and word documents.	Access restricted Admissions Officer/SBM/Admin	Information is shared with SLT, Local authority; emergency services where required incase of emergency	Primary - Retain for time which pupil remains at school. Transfer to secondary or other primary when child leaves.	Restricted authorised only access to files; Secure, locked storage; Information kept on site at all times Password protected electronic files; Regular review and update of information for accuracy and relevance; Effective archiving and deletion procedures.	Yes
	10	Waiting lists	Enrolment details, including name, home address, Birth Cert, Baptisam Cert, Proof of Address, Religion, parents'/carers' details, confirmation of parental responsibility;	- To ensure child correctly ranked/placed in school - To meet Local Authority Requirments - To ensure Admissions Policy adhered to - To meet school requirements	- Consent - Contract - Public Task	Paper Documents stored in secure, fixed filing cabinet onsite. Archived information stored in locked cupboard	Admissions Officer/SBM/Admin	0 Current Files 0 Archived Files Total 0	Yes	Paper files stored in secure locked filing cabinet.	Access restricted Admissions Officer/SBM/Admin	Information shared with Local Authority and SENCO where required		Secure, locked storage; Information kept onsite at all times. Regular review amd update of information for accuracy and relevance.	Yes
	11	Attendance Registers	Information on children's attendance, including dates and times of arrival and departure.	- To meet Local Authority Requirements - To meet school requirements	- Consent - Contract - Legal Obligation - Public Task	Password protected system; Archived information stored in locked cupboard	Attendance/ Admissions Officer		Yes	Password protected system	Restricted Access	Information shared with Local Authority/SENCO/ OfSted/ where required	3yrs	Password protected electronic file; Restricted access;	Yes
	12	SEND information	Can include learning journey information, summative assessments, individual education plans, health care plans, individual risk assessments, referrals, Early Help Assessments, and medical records.	- To meet Local Authority Requirements - To meet school requirements - To provide support	- Consent - Contract - Legal Obligation - Public Task	Archived information stored in locked cupboard; Paper documents stored in secure, fixed filing cabinet on site; Password protected system	SENCO TEAM	88 Current Files 25 Archived Files Total 113	Yes	Paper files stored in secure locked filing cabinet; Password protected Integris system, and word documents.	Restricted Access	Information shared with Local Authority/SENCO/ OfSted/ where required	DOB of Pupil +25yrs	Restricted authorised only access to files; Secure, locked storage; Information kept on site at all times Password protected electronic files; Regular review and update of information for accuracy and relevance; Effective archiving and deletion procedures.	Yes

	13	Child Protection files	Child protection information, referrals, minutes, child protection/in need plan and court reports and orders. Generally highly confidential information.	- To meet Local Authority Requirements - To meet school requirements - To provide support	- Consent - Contract - Legal Obligation - Public Task	Paper Documents stored in secure, fixed filing cabinet onsite. Archived information stored in locked cupboard	SLT/Restrcited Admin	37 Current Files 9 Archived Files Total 46	Yes	Paper files stored in secure locked filing cabinet; Password protected Integris system, and word documents.	Restricted Access	Information shared with Local Authority/SENCO/ OfSted/ where required	DOB of Pupil +25yrs	Restricted authorised only access to files; Secure, locked storage; Information kept on site at all times Password protected electronic files; Regular review and update of information for accuracy and relevance; Effective archiving and deletion procedures.	Yes
	14	Accident records	Information relating to accidents and injuries occurring in the setting. Can also include accidents involving staff or third parties.	- To meet Local Authority Requirements - To meet school requirenments - To obtain accurate account of incident	- Consent - Contract - Legal Obligation - Vital Interest - Public Task - Legitimate Interest - Consent - Contract - Legal Obligation	Paper Documents stored in secure, fixed filing cabinet onsite. Archived information stored in locked cupboard	First Aid Lead	1 Current Book 3 Archived books Total 4	Yes	Paper Documents stored in secure, fixed filing cabinet onsite.	All Staff	Information is shared with senior managers, Ofsted and the local authority where required for safeguarding and child protection purposes.	DOB of Pupil +25yrs	Secure, locked storage; Information kept onsite at all times.	Yes
SUPPLIERS/ MAINTENANCE CONTRACTORS'	15	Business information	Contact details; contract details; and financial information;	- To meet Local Authority Requirements - To meet school requirements	- Consent - Contract - Legal Obligation - Public Task - Legitiment Interest	Password protected system; Archived information stored in locked cupboard	SBM		Yes	Password protected system	Restricted Access	Information shared with Diocese/Local Authority where need be	6years	Secure, locked storage; Information kept onsite at all times.	Yes

GENERAL	16	Computer systems	Management of setting, including parent and child details, financial information, business information, learning and development records, headcount information and more.	- To meet Local Authority Requirements - To meet school requirements	- Consent - Contract - Legal Obligation - Public Task - Legitiment Interest	Password protected system; Computer files held on cloud;	IT Dept/Head		Yes	Password protected system	Access dependent on information. Different levels of access for different staff	Information shared with Local Authority/Dioceses/ Ofsted when required for safeguarding and child protection purposes.	Refer to retention time of specified information	Restricted authorised only access to files; Secure, locked storage; Information kept on site at all times Password protected electronic files; Regular review and update of information for accuracy and relevance; Effective archiving and deletion procedures.	Yes
	17	Complaints	A complaint log maintained to record any complaint. Separate in depth logs and notes from investigations for written and more complex complaints. Additional logs may be maintained of complaints regarding other issues.	- To meet Local Authority Requirements - To meet school requirements	- Consent - Contract - Legal Obligation - Public Task - Legitiment Interest	Password protected system; Paper Documents stored in secure, fixed filing cabinet onsite. Archived information stored in locked cupboard	SLT/SBM	0 Active Files 0 Archived Files Total 0	Yes	Paper files stored in secure locked filing cabinet; Password protected Integris system, and word documents.	Restricted Access	Information shared with Local Authority/Dioceses/ Ofsted when required	Resolution date +6yrs	Restricted authorised only access to files; Secure, locked storage; Information kept on site at all times Password protected electronic files;	

Data Protection Breach Reporting Form

1. Summary of Incident

Date and Time of Incident:	
Number of people whose date is affected:	
Department:	
Nature of breach: **e.g. Theft/disclosed in error/technical problem**	
Description of how breach occurred:	

2. Reporting

When was breach reported?	
How did you become aware of the breach?	
Has DPC and DPO been informed? **DPC – Patrick Devereux** **DPO – Lucy Henderson**	

Sections 3 to 6 are to be completed by DPC/DPO

3. Personal Data

Full description of personal data involved (without Identifiers);	
Number of individuals affected:	
Have all affected individuals been informed?	
If not, state why not:	
Is there any evidence to date that the personal data involved in this incident has been inappropriately processed or further disclosed? If so, please provide details:	

4. Data Retrieval

What immediate remedial action was taken:	
Has the data been retrieved or deleted? If yes – date and time:	

5. Impact

Describe the risk of harm to the individual as a result of this incident:	
Describe the risk of identity fraud as a result of this incident:	
Have you received a formal complaint from any individual affected by this breach? Is, provide details:	

6. Management

Do you consider the employee(s) involved has breached information governances policies and procedures:	
Please inform of any disciplinary action taken in relation to the employee(s) involved:	
Had the employee(s) completed GDPR training?	
As a result of this incident, do you consider whether any other personal data held may be exposed to similar vulnerabilities? If so, what steps have been taken to address this:	

Has there been any media coverage if the incident? If so, please provide details:	
What further action has been taken to minimise the possibility of a repeat of such an incident? Please provide copies of any internal correspondence regarding any changes in procedure:	