Lanesend Primary School

Data Protection Policy Including GDPR and Management of School Records 2022

Statutory Policy

Signed: ..... Date:
(Headteacher)

Signed: ..... Date:
(Chair of Trustees)

Review Date: January 2023 (Yearly)
Reviewed By: Headteacher, School Finance Manager and Board of Trustees

Lanesend Primary School
Data Protection, GDPR and Management of School Records Policy

The Data Protection Act 1998 is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the Data Protection Act. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

1. Scope of the Policy

Personal information is any information that relates to a living individual who can be identified from the information. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

The School collects a large amount of personal data every year including: staff records, names and addresses of those requesting a prospectus, assessment results, references, fee collection as well as the many different types of research data used by the School. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

2. The Eight Principles

The Act is based on eight data protection principles, or rules for 'good information handling'.

1. Data must be processed fairly and lawfully.

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

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.

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

5. Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose.

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

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

8. Personal data shall not be transferred to a country outside the EEA, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

3. Responsibilities

3.1 The school must:
Manage and process personal data properly
Protect the individuals right to privacy
Provide an individual with access to all personal data held on them.

3.2 The school has a legal responsibility to comply with the Act. The school, as a corporate body, is named as the Data Controller under the Act.

Data Controllers are people or organisations who hold and use personal information. They decide how and why the information is used and have a responsibility to establish workplace practices and policies that are in line with the Act.

3.3 The school is required to 'notify' the Information Commissioner of the processing of personal data. This information will be included in a public register which is available on the Information Commissioner's website at the following link: https://ico.org.uk/

3.4 Every member of staff that holds personal information has to comply with the Act when managing that information.

3.5 The school is committed to maintaining the eight principles at all times. This means that the school will:

- inform Data Subjects why they need their personal information, how they will use it and with whom it may be shared. This is known as a Privacy Notice ***(see Appendix 2).***

- check the quality and accuracy of the information held

- apply the records management policies and procedures to ensure that information is not held longer than is necessary

- ensure that when information is authorised for disposal it is done appropriately

- ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system

- only share personal information with others 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 in the Data Protection Act ***(see Appendix 1)***

- train all staff so that they are aware of their responsibilities and of the schools relevant policies and procedures

This policy will be updated as necessary to reflect best practice or amendments made to the Data Protection Act 1998.

Please follow this link to the ICO's website (https://ico.org.uk/) which provides further detailed guidance on a range of topics including individuals' rights, exemptions from the Act, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc. In particular, you may find it helpful to read the Guide to Data Protection which is available from the website.

Personal data protection and GDPR

The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government.

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Under the Data Protection Act 2018, you have the right to find out what information the government and other organisations store about you. These include the right to:

- be informed about how your data is being used
- access personal data
- have incorrect data updated
- have data erased
- stop or restrict the processing of your data
- data portability (allowing you to get and reuse your data for different services)

- object to how your data is processed in certain circumstances

You also have rights when an organisation is using your personal data for:

- automated decision-making processes (without human involvement)
- profiling, for example to predict your behaviour or interests

A Subject Access Request needs to follow the GDPR Policy and does not fall under Freedom of Information.

Subject Access Requests

This section explains your Rights to see personal information we keep and how you can access it.

Why is personal Information held?

So that we can fulfill all safeguarding and legal requirements regarding our children and their families.

How is information kept and who is responsible?

The information is kept secure on our computer systems and files; the responsibility to keep your information secure is maintained by the school. This includes retention and destruction of the information.

The school's employees have a duty of care where applicable to you, which includes respecting your right to confidentiality and ensuring that information is only used and given to others for the purpose of the service being provided.

Who is the information shared with?

Information you provide may also be shared with other schools or agencies involved in the provision of services to your child, where you have agreed to this at the time of providing us with your information or where we are legally permitted to do so. The information will only be the minimum necessary to enable us to provide services to you. Please note, we will only share information with other agencies such as the police, where there is a justified reason to do so for safeguarding purposes.

Do I have the right to see my information?

You have the right to request access to information that the school holds about you, where the information relates to you or your child. However, where records contain data about another person, even if it is a member of your own family, you will not be able to see this information.

How can I access my personal information?

Requests should be made in writing and provide as much information as possible i.e. Full name, date of birth, current and previous address/es. All requests should be sent to the Data Protection Officer.

Identification is also required, such as a driving license, utility bill or some other documentation to provide us evidence of who you are and your current address. Once we have received all the relevant information from you under the General Data Protection Regulation we have 1 calendar month to respond to your request. For large and/or complex requests this time limit may be extended by an additional 2 months.

Further Information on Data Protection Legislation can be obtained from The Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF 01625 www.ico.gov.uk

Privacy Notices

Employment Privacy Notice

Introduction

Lanesend Primary ("the Company") is committed to protecting the privacy and security of your personal information.

This employment privacy notice describes how we collect and use personal information about you before, during and after your working relationship with us, in accordance with the General Data Protection Regulation known as GDPR.

It applies to all employees, workers and contractors.

The Company is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under the GDPR to notify you of the information contained in this employment privacy notice.

This notice does not form part of any contract of employment or other contract to provide services. We may amend or update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Data Protection Principles

We will comply with data protection law. In summary this says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.

2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.

3. Relevant to the purposes we have told you about and limited only to those purposes.

4. Accurate and kept up to date.

5. Kept only as long as necessary for the purposes we have told you about and kept securely.

Information Held

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data). There are "special categories" of more sensitive personal data which require a higher level of protection (see below).

Employees, Workers & Contractors

If you become an employee, worker or contractor of the Company, we will collect, store, and use some or all of the following categories of personal information about you:

- Personal contact details such as name, title, postal address, telephone numbers, and a personal email address
- Date of birth
- Gender
- Marital status and dependants
- Next of kin and emergency contact information
- National Insurance number
- Bank account details, payroll records and tax status information
- Salary, annual leave, pension and benefits information
- Start date
- Location of employment or workplace
- Copy of driving licence
- Motor vehicle details, insurance and driving licence details for those who use cars for business use
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process)
- Employment records (including job titles, work history, working hours, training records and professional memberships)
- Accident records
- Compensation history
- Performance information
- Information relating to work attendance and absence and punctuality
- Disciplinary and grievance information
- Information about your use of our information and communications systems

- Photographs

We may also collect, store and use the following "special categories" of more sensitive personal information:

- Trade union membership
- Information about your health, including any medical condition, health and sickness records
- Information about criminal convictions and offences

Collection of Personal Information

We collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers or other background check agencies.

We will collect additional personal information in the course of job-related activities throughout the period of your working for us.

We may also collect limited personal information relating to members of your family or a partner where this is required so that we have contact details for next of kin in the event or an emergency.

Use of Personal Information

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you.

2. Where we need to comply with a legal obligation.

3. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare: (1) Where we need to protect your interests (or someone else's interests); or (2) Where it is needed in the public interest or for official purposes.

We need all the categories of information in the list above to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below.

- Making a decision about your recruitment or appointment
- Determining the terms on which you work for us
- Checking you are legally entitled to work in the UK
- Paying you and, if you are an employee, deducting tax and National Insurance contributions
- Providing employment benefits to you such as a car allowance, private medical insurance, death in service cover, pension, bonus and commission
- Liaising with your pension provider
- Administering the contract we have entered into with you
- Business management and planning, including accounting and auditing
- Conducting performance reviews, managing performance and determining performance requirements
- Making decisions about salary reviews and compensation
- Assessing qualifications for a particular job or task, including decisions about promotions
- Gathering evidence for possible grievance or disciplinary hearings
- Making decisions about your continued employment or engagement
- Making arrangements for the termination of our working relationship
- Education, training and development requirements
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work
- Ascertaining your fitness to work
- Managing sickness absence
- Complying with health and safety obligations
- To prevent fraud
- To monitor your use of our information and communication systems to ensure compliance with our IT policies
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution
- To conduct data analytics studies to review and better understand employee retention and attrition rates
- Equal opportunities monitoring.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

Failure to Provide Personal Information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of Purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Use of Sensitive Personal Information

The "special categories" of sensitive personal information referred to above require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.

2. Where we need to carry out our legal obligations and in line with our data protection policy.

3. Where it is needed in the public interest, such as for equal opportunities monitoring and in line with our data protection policy.

4. Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Our Obligations as Employer

We will use your particularly sensitive personal information in the following ways:

- We will use information relating to leave of absence, which may include sickness absence or family related leave, to comply with employment and other laws.
- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.
- We will use trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.

Consent

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about Criminal Convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We do envisage that we will hold information about criminal convictions.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We will use information about criminal convictions and offences in the following ways:

- Assessing your suitability for employment.
- Making decisions about your continued employment or engagement.
- Ensuring compliance with safeguarding legislation where relevant.

We are allowed to use your personal information in this way where it is necessary to carry out employment rights and obligations and provided we do so in line with our data protection policy.

Data Sharing

We may have to share your data with third parties, including third-party service providers.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the EU. If we do, you can expect a similar degree of protection in respect of your personal information.

Third Parties

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

"Third parties" includes third-party service providers (including contractors and designated agents) and other entities. The following activities are carried out by third-party service providers: HR, Payroll, pension administration, benefits provision and administration, IT services.

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. Data is provided to our third party service providers for specified purposes and not for use for their own purposes.

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. We may also need to share your personal information with a regulator or to otherwise comply with the law.

Data Security

We have put in place appropriate measures to protect the security of your information.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data Retention

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of

the Company we will retain and securely destroy your personal information in accordance with applicable laws and regulations.

Rights of Access, Correction, Erasure & Restriction

Duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Rights in connection with personal information

Under certain circumstances, by law you have the right to:

- Request access to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground.
- Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- Request the transfer of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the School Finance Manager in writing.

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Withdrawing Consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Company Secretary. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Complaints

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

Changes to this Employment Privacy Notice

We reserve the right to update this employment privacy notice at any time, and we will advise you of any substantial updates and provide you with access to a new employment privacy notice. We may also notify you in other ways from time to time about the processing of your personal information.

Queries

If you have any questions about this employment privacy notice or how we handle your personal information, please contact the School Finance Manager.

Privacy Notice (How we use pupil information)

Lanesend Primary is the Data Controller for personal information with respect to responsibility under Data protection legislation.

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information (such as national curriculum assessment results)

- Relevant medical information
- Information relating to special educational needs
- Behavioural information and exclusions
- Safeguarding

Why we collect and use this information
We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing

The lawful basis on which we use this information

Lanesend Primary School holds the legal right to collect and use personal data relating to pupils and their families, and we may also receive information regarding them from their previous school, LA and/or the DfE. This information is needed to enable us to comply with our legal obligation to provide an education service. We collect and use personal data in order to meet legal requirements including:

- Education Act 1996
- The Education (Information About Individual Pupils) (England) Regulations 2013
- Keeping Children Safe in Education 2016
- Working Together to Safeguard Children 2015

Who we share pupil information with

We routinely share pupil information with:

- schools that the pupils attend after leaving us
- our local education authority
- the Department for Education (DfE)
- school nurse, NHS, CAMHS, Pediatricians,
- NHS health care and Childrens Services including speech therapy, physiotherapy, occupational therapy, educational psychologist (once consent was gained)
- Educational Psychologists
- Childrens Services, including Safeguarding

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with Data Protection legislation, we will inform you whether you are required to provide certain pupil information to us or if your consent is needed. Where consent is required, we will provide you with specific information with regards to the reasons the data is being collected and how the data will be used.

Storing pupil data

Personal data relating to pupils at school and their families is stored in line with our Data Protection Policy.
In accordance with the Data Protection Policy, the school does not store personal data indefinitely; data is only stored for as long as is necessary to complete the task for which it was originally collected. Details of the retention of records can be found in our Retention Policy

Why we share pupil information

We only share personal data where the law requires us to do so or where we obtain consent.
We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.
We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013 and also Keeping Children Safe in Education 2016 and Working Together to Safeguard Children 2015.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.
The National Pupil Database (NPD) is owned and managed by the Department for Education and contains information about pupils in schools in England. We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The DfE may share information about our pupils from the NDP with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The DfE has robust processes in place to ensure the confidentiality of personal data is maintained.
For more information about the DfE's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data
To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, parents and pupils have certain rights with respect to their personal data.
You have the right to:

- apply to request access to information that we hold about them
- object to processing of personal data that is likely to cause, or is causing, damage or distress
- restrict processing for certain purposes, e.g. direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, restrict its processing, erased or destroyed; and
- data portability

For further details on your rights or to apply to access your personal information, or be given access to your child's educational record, contact School Office Manager, Lanesend Primary School, Love Lane, Cowes, Isle of Wight, PO31 7ES Tel 01983 293233 or email office.manager@lanesendpri.iow.sch.uk

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. School Office Manager, Lanesend Primary School, Love Lane, Cowes, Isle of Wight, PO31 7ES Tel 01983 293233 or email office.manager@lanesendpri.iow.sch.uk You also have the right to raise concerns with the school's Data Protection Officer; the Head of Legal Services and Monitoring Officer at the Isle of Wight Council, dpo@IOW.gov.uk. Ultimately, you also have the right to contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact:
School Office Manager, Lanesend Primary School, Love Lane, Cowes, Isle of Wight, PO31 7ES Tel 01983 293233 or email office.manager@lanesendpri.iow.sch.uk

Guidance on the Reuse of Information

Lanesend Primary School allows the re-use of information in accordance with the terms and conditions of the Open Government Licence
http://www.nationalarchives.gov.uk/doc/open-government-licence/version/2/

Management of School Records

The School recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the school. Records provide evidence for protecting the legal rights and interests of the school, and provide evidence for demonstrating performance and accountability.

All records are created, received or maintained by staff of the school in the course of carrying out its functions.

Records are defined as all those documents which facilitate the business carried out by the school and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created or received, and then stored, in hard copy or electronically.

A small percentage of the school's records may be selected for permanent preservation as part of the institution's archives and for historical research.

The school has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Headteacher, and assisted by each team manager, so they are responsible for their records and the appropriate management of them.

Each member of staff responsible for record management in the school will be advised by the Headteacher or School Finance Manager regarding good record management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately.

Individual staff and employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the school's records management guidelines.

Recording Systems

Information created by the school must be managed against the same standards regardless of the media in which it is stored.

Maintenance of Record Keeping Systems

It is important that filing information is properly resourced and is carried out on a regular basis. It is equally important that the files are weeded of extraneous information where appropriate on a regular basis. Removing information from a file once a freedom of information request has been made will be a criminal offence (unless it is part of normal processing).

Applying retention periods is straightforward provided files are closed on a regular basis.

Once a file has been closed, it should be moved out of the current filing system and stored in archived boxes and stored in the archived shelving at the back of the garages, until it has reached the end of the retention period.

Information security is very important especially when dealing with personal information or sensitive policy information. There are a number of basic rules:

- All personal information should be kept in lockable filing cabinets which are kept locked when the room is unattended;

- Personal information held on computer systems should be adequately password protected.
Information should never be left up on a screen if the computer is unattended;

- Files containing personal or sensitive information should not be left out on desks over night;

- Where possible sensitive personal information should not be sent by e-mail;

- If files need to be taken off the premises they should be secured in the boot of a car

- All computer information should be backed up regularly and the back-up is stored both on and off site.

v. Information contained in email should be filed into the appropriate electronic or manual filing system once it has been dealt with.

Transfers to receiving schools, either in year or at Secondary Transition point

The pupil record should not be weeded before transfer to the secondary school unless any records with a short retention period have been placed in the file. It is important to remember that the information which may seem unnecessary to the person weeding the file may be a vital piece of information required at a later stage.

Primary schools do not need to keep copies of any records in the pupil record except if there is an ongoing legal action when the pupil leaves the school or if the child has

been on a Child Protection Plan. Custody of and responsibility for the records passes to the school the pupil transfers to.

If files are sent by post, they should be sent by registered post with an accompanying list of the files. Where possible, the receiving school should sign a copy of the list to say that they have received the files and return that to the primary school. Where appropriate, records can be delivered by hand with signed confirmation for tracking and auditing purposes. **Please see Appendix 6.**

Electronic documents that relate to the pupil file also need to be transferred, or, if duplicated in a master paper file, destroyed.

The Safe Disposal of Information Using the Retention Schedule

Files should be disposed of in line with the attached retention schedule (see Appendix 2). This is a process which should be undertaken on an annual basis during the month of August.

Paper records containing personal information should be shredded using a cross-cutting shredder. Other files can be burnt or given to a confidential shredder provider. Loose papers should not be put in skips unless the skip has a lid. USB sticks will be wiped and reset.

Electronic data should be archived on electronic media and 'deleted' appropriately at the end of the retention period.

Data Breach

Lanesend Primary School holds large amounts of data including personal data relating to children, families and staff. The school is considered the data controller for all personal data that it processes, and, as such, it has responsibilities to ensure that all data is processed securely and in accordance with the requirements of relevant data protection legislation.
Every care is taken to protect personal data and to ensure that it is only shared with those who are entitled to access it. However, in the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible.

This applies to all personal and sensitive data held by the school. All staff are required to comply with these procedures. Disciplinary action may be taken against staff who fail to ensure the safe and secure processing of personal data.

The Information Commissioners Office (ICO) has the power to take enforcement action against any organisation that breaches data protection legislation. Under the General Data Protection Regulation (GDPR), that comes into effect in May 2018,

these powers are extended to include the ability to impose fines of up to 4% of gross turnover or 20 million euros.

Definition - What is a Personal Data Breach?

A “personal data breach” is defined as:

“a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.”

A breach is a type of security incident. Whilst all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches.
The consequence of a personal data breach is where the council is unable to ensure compliance with the data protection principles.

Breaches can be categorised according to the following principles:

- “Confidentiality breach” - where there is an unauthorised or accidental disclosure of, or access to, personal data.
- “Integrity breach” - where there is an unauthorised or accidental alteration of personal data.
- “Availability breach” - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

Types of Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

Breaches can be caused by a number of factors:

- Loss or theft of papers/files/data and/ or equipment on which data is stored;
- Inappropriate access to records, allowing unauthorised use;
- Human error;
- Equipment failure;
- Poor data destruction procedures;

- Cyber-attack;
- Hacking.

Reporting incidents

All complaints, suspected breaches/incidents should be reported to The Isle of Wight Council immediately.

There is a data breach incident reporting form (see Appendix A) to assist staff in reporting incidents. This form should be completed as soon as possible after the breach is reported by the Data Protection Officer. Where information has been sent to, or given to, the wrong recipient, efforts should be made to retrieve the data as soon as possible, where it is safe to do so. The prompt retrieval of information will limit the harm caused and mitigate the risk

The Isle of Wight Council Data Protection Officer will complete an investigation, on behalf of the school. The investigation may involve a referral to HR where the actions of a member of staff have caused the breach, and will involve liaising with various colleagues in ICT, legal etc for suitable advice.
In considering the seriousness of the incident, consideration will be taken of:

- The type of breach;
- The nature, sensitivity and volume of personal data;
- Ease of identification of individuals;
- Severity of consequences for individuals;
- Special characteristics of the individuals;
- The number of affected individuals.

Determining the level of a breach

To assist in assessing the level of risk involved in a breach, the council will continue to use the scoring matrix recommended by the IG Toolkit Incident Reporting Tool (see Appendix B). Where incidents result in a Level 1 or above breach, a self-referral will be made to the ICO unless it is determined that it is unlikely to result in a risk to the rights and freedoms of an individual (as stipulated by the GDPR).

Self reporting to the Information Commissioners Office (ICO)

The General Data Protection Regulation (the GDPR) introduces the requirement for a personal data breach to be notified to the competent national supervisory authority, which in the UK is the Information Commissioners Office (ICO) and, in certain cases, to communicate the breach to the individuals whose personal data have been affected by the breach.

The school must report all data breaches to the ICO without undue delay and, where feasible, not later than 72 hours after having become aware of it unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where it is not possible to report within the 72 hours, we must provide reasons for the delay.

Certain information must be provided when reporting a data breach to the ICO, this includes:
"(a) nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
(b) the name and contact details of the data protection officer or other contact point where more information can be obtained;
(c) describe the likely consequences of the personal data breach;
(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects."

It is recognised that, depending on the nature of a breach, further investigation may be necessary to establish all of the relevant facts relating to the incident. Information may be provided in phases where further details are identified following investigation, but every effort should be made to report as soon as the school becomes aware that a breach may have occurred.

Examples:

- A family member informs the school that they have accidentally received a letter addressed to another family that includes personal data. The date the family member informed the school is the date that we were made aware.

- The school detects that there has been a possible intrusion into its network. The systems are checked to establish whether personal data held on that system has been compromised and confirms this is the case – this is the date that the school is aware of the breach.

- A cybercriminal contacts the school after having hacked its system in order to ask for a ransom. In that case, after checking its system to confirm it has been attacked, the school has clear evidence that a breach has occurred and there is no doubt that it has become aware.

After first being informed of a potential breach or when it has itself detected a security incident, the school may undertake a short period of investigation in order to establish whether or not a breach has in fact occurred. During this period of investigation the school may not be regarded as being "aware". However, it is expected that the initial investigation should begin as soon as possible and establish with a reasonable degree of certainty whether a breach has taken place; a more detailed investigation can then follow.

Informing individuals

The school is required to inform data subjects of a data breach, “When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons”. The communication of a breach to individuals should be made “without undue delay,” i.e. as soon as possible. The main objective of notification to individuals is to provide specific information about steps they should take to protect themselves. There are 3 situations where controllers are not required to notify individuals of a breach:

- The controller has applied appropriate technical and organisational measures to protect personal data prior to the breach, in particular those measures that render personal data unintelligible to any person who is not authorised to access it. This could, for example, include protecting personal data with state-of-the-art encryption, or by tokenization.

- Immediately following a breach, the controller has taken steps to ensure that the high risk posed to individuals’ rights and freedoms is no longer likely to materialise. For example, depending on the circumstances of the case, the controller may have immediately identified and taken action against the individual who has accessed personal data before they were able to do anything with it. Due regard still needs to be given to the possible consequences of any breach of confidentiality, again, depending on the nature of the data concerned.

- It would involve disproportionate effort to contact individuals, perhaps where their contact details have been lost as a result of the breach or are not known in the first place. In the case of disproportionate effort, technical arrangements could also be envisaged to make information about the breach available on demand, which could prove useful to those individuals who may be affected by a breach, but the controller cannot otherwise contact.

Documenting breaches

Regardless of whether or not a breach needs to be notified to the Council or CIU, the school must keep details of all breaches, including the facts relating to the breach, its effects and any remedial action taken. The Council and Corporate Information Unit will maintain a log of all breaches.

Advice and guidance on all matters relating to data protection legislation and confidentiality can be obtained by contacting the Corporate Information Unit, ciu@iow.gov.uk.

Appendix 2 - Management of School Records Retention Schedule

Child Protection

The retention and use of records relating to child protection matters concerning pupils, and child protection allegations against staff requires specific guidance in this schedule. This will be subject to updates following implementation of recommendations by legislation.

Basic File Description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
Child Protection files including CAF files	Yes	Education Act 2002, s175, related guidance 'Safeguarding Children in Education', September 2004	DOB + 25 years	File transferred to receiving school SECURE DISPOSAL at end of retention period.
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 the person's normal retirement age, or 10 years from the date of the allegation if that is longer	SECURE DISPOSAL

Governors

Basic File Description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
Minutes				
§ Principal set (signed)	No		Permanent	Retain in school for 6 years from date of meeting
§ Inspection Copies	No		Date of meeting + 3 years	SECURE DISPOSAL [If these minutes contain any sensitive personal information they must be shredded]
Agendas	No		Date of meeting	SECURE DISPOSAL
Reports	No		Date of report + 6 years	Retain in school for 6 years from date of meeting
Instruments of Government	No		Permanent	Retain in school whilst school is open
Trusts	No		Permanent	Retain in school whilst operationally required
Action Plans	No		Date of action plan + 3 years	SECURE DISPOSAL
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)
Complaints files	Yes		Date of resolution of complaint + 6 years	Retain in school for the first six years. Review for further retention in the case of contentious disputes. SECURE DISPOSAL routine complaints.
Annual Reports required by the Department for Education	No	Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002.S1 2002 No 1171	Date of report + 10 years	

Management				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
Log Books [Books where the Headteacher or another member of staff keeps a record of what happens in the school, this may include details of events, photographs and other information]	Yes		Date of last entry in the book + 6 years	Retain in the school for 6 years from the date of the last entry
Minutes of Progression Team meetings and other internal administrative bodies	Yes		Date of meeting + 5 years	Retain in the school for 5 years from meeting
Reports made by the Headteacher or the management team	Yes		Date of report + 3 years	Retain in the school for 3 years from meeting
Records created by head teachers, deputy head teachers, phase leaders and other members of staff with administrative responsibilities.	Yes		Closure of file + 6 years	SECURE DISPOSAL
Correspondence created by Headteachers, deputy Headteachers, phase leaders and other members of staff with administrative responsibilities	No		Date of correspondence + 3 years	SECURE DISPOSAL
Professional development plans	Yes		Closure + 6 years	SECURE DISPOSAL
School Development Plans	Yes		Closure + 6 years	Review

Pupils				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
Admission Registers	Yes		Date of last entry in SIMs + 6 years	Retain in the school for 6 years from the date of the last entry then consider transfer to the archives.
Attendance registers	Yes		Date of register + 3 years	SECURE DISPOSAL [If these records are retained electronically any back up copies should be destroyed at the same time]
Pupil record cards	Yes			
§ Primary			Retain for the time which the pupil remains at the primary school	Transfer to the secondary school (or other primary school) when the child leaves the school.
Pupil files	Yes			
§ Primary			Retain for the time which the pupil remains at the primary school	Transfer to the Secondary school (or other primary school) when the child leaves the school.
Additional Educational Needs files, reviews and Personal Education Plans, Education, Health and Care plans,	Yes		DOB of the pupil + 25 years then 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.	Transfer to the Secondary school (or other primary school) when the child leaves the school.
Correspondence Relating to Authorised Absence and Issues	No		Date of absence + 2 years	SECURE DISPOSAL or Transfer to the Secondary school (or other primary school) when the child leaves the school.
Examination results	Yes			
§ Public	No		Year of examinations + 6 years	SECURE DISPOSAL or Transfer to the Secondary school (or other primary school) when the child leaves the school.
§ Internal examination results	Yes		Current year + 5 years [(2)]	SECURE DISPOSAL or Transfer to the Secondary school (or other primary school) when the child leaves the school.
Any other records created in the course of contact with pupils	Yes/No		Current year + 3 years	Review at the end of 3 years and either allocated a further retention period or SECURE DISPOSAL or Transfer to the Secondary school (or other primary school) when the child leaves the school.
Statement or EHC Plan maintained under The Education Act	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	SECURE DISPOSAL unless legal action is pending

[(2)] 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.

Pupils cont'd.				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
Proposed statement or amended statement	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	SECURE DISPOSAL unless legal action is pending
Advice and information to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Closure + 12 years	SECURE DISPOSAL unless legal action is pending or Transfer to the Secondary school (or other primary school) when the child leaves the school.
Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Closure + 12 years	SECURE DISPOSAL unless legal action is pending
Parental permission slips for school trips – where there has been no major incident	Yes		Conclusion of the trip	SECURE DISPOSAL
Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980	DOB of the pupil involved in the incident + 25 years. The permission slips for all pupils on the trip need to be retained to show that the rules had been followed for all pupils.	SECURE DISPOSAL

Curriculum				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
School Development Plan	No		Current year + 6 years	SECURE DISPOSAL
Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL
Schemes of work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
Timetable	No		Current year + 1 year	SECURE DISPOSAL
Class record books	No		Current year + 1 year	SECURE DISPOSAL
Mark Books	No		Current year + 1 year	SECURE DISPOSAL
Record of Homework set	No		Current year + 1 year	SECURE DISPOSAL
Samples of Pupils work	No		Current year + 1 year	SECURE DISPOSAL
Examination results	Yes		Current year + 6 years	SECURE DISPOSAL
SATS records – Examination Papers and Results	Yes		Current year + 6 years	SECURE DISPOSAL
PAN reports	Yes		Current year + 6 years	SECURE DISPOSAL
Value Added & Contextual Data	Yes		Current year + 6 years	SECURE DISPOSAL

Self-Evaluation forms	Yes		Current year + 6 years	SECURE DISPOSAL

Personnel				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
Timesheets, sick pay	Yes	Financial Regulations	Current year + 6 years	SECURE DISPOSAL
Staff Personal files	Yes		Termination + 7 years	SECURE DISPOSAL
Interview notes and recruitment records	Yes		Date of interview + 6 months	SECURE DISPOSAL
Pre-employment vetting information (including unsuccessful DBS checks)	No	DBS guidelines	Date of check + 6 months	SECURE DISPOSAL [by the designated member of staff]
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.		
§ Oral warning			Date of warning + 6 months	SECURE DISPOSAL If this is placed on a personal file, it must be weeded from the file
§ Written warning – level 1			Date of warning + 6 months	SECURE DISPOSAL If this is placed on a personal file, it must be weeded from the file
§ Written warming – level 2			Date of warning + 12 months	SECURE DISPOSAL If this is placed on a personal file, it must be weeded from the file
§ Final warning			Date of warning + 18 months	SECURE DISPOSAL If this is placed on a personal file, it must be weeded from the file
§ Case not found			If child protection related please see 1.2, otherwise SECURE DISPOSAL immediately at the conclusion of the case	
Records relating to accident/injury at work	Yes		Date of incident + 12 years In the case of serious accidents a further retention period will need to be applied.	SECURE DISPOSAL
Annual appraisal/assessment records	No		Current year + 5 years	SECURE DISPOSAL
Maternity pay records	Yes	Statutory Maternity Pay (General Regulations1986 (SI 1986/1990), revised 1999 (SI 1999/567)	Current year + 3 years	SECURE DISPOSAL
Records held under Retirement Benets Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SECURE DISPOSAL
Proofs of identity collected as part of the process of checking "portable" enhanced DBS 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.	

Health and Safety				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
Accessibility Plans		Disability Discrimination Act	Current year + 6 years	SECURE DISPOSAL
Accident Reporting		Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980.		
§ Adults	Yes		Date of incident + 7 years	SECURE DISPOSAL
§ Children	Yes		DOB of child + 25 years [3]	SECURE DISPOSAL
COSHH			Current year + 10 years [Where appropriate an additional retention period may be allocated]	
Incident reports	Yes		Current year + 20 years	SECURE DISPOSAL
Policy Statements			Date of expiry + 1 year	SECURE DISPOSAL
Risk Assessments	Yes		Current year + 3 years	SECURE DISPOSAL
Process of monitoring of areas where employees and persons are likely to have come in contact with asbestos			Last action + 40 years	SECURE DISPOSAL
Process of monitoring of areas where employees and persons are likely to have come in contact with radiation			Last action + 50 years	SECURE DISPOSAL
Fire Precautions log books			Current year + 6 years	SECURE DISPOSAL

[3] 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.

Administrative				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
Employer's Liability Certificate			Closure of the school + 40 years	SECURE DISPOSAL
Inventories of equipment and furniture			Current year + 6 years	SECURE DISPOSAL
General file series			Current year + 5 years	Review to see whether a further retention period is required
School brochure/prospectus			Current year + 3 years	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
Circulars (staff/parents/pupils)			Current year + 1 year	SECURE DISPOSAL
Newsletters, ephemera			Current year + 1 year	Review to see whether a further retention period is required
Visitors' log			Current year + 2 years	Review to see whether a further retention period is required
LEAF (Lanesend Active Families)			Current year + 6 years	Review to see whether a further retention period is required

Finance				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
Annual Accounts		Financial Regulations	Current year + 6 years	Archive
Loans and grants		Financial regulations	Date of last payment on loan + 12 years	Review to see whether a further retention period is required
Contracts				
§ Under seal			Contract completion date + 12 years	SECURE DISPOSAL
§ Under signature			Contract completion date + 6 years	SECURE DISPOSAL
§ Monitoring records			Current year + 2 years	SECURE DISPOSAL
Copy orders			Current year + 2 years	SECURE DISPOSAL
Budget reports, budget monitoring etc.			Current year + 3 years	SECURE DISPOSAL

Finance cont'd.				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
Invoice, receipts and other records covered by the Financial Regulations		Financial Regulations	Current year + 6 years	SECURE DISPOSAL
Annual Budget and background papers			Current year + 6 years	SECURE DISPOSAL
Order books and requisitions			Current year + 6 years	SECURE DISPOSAL
Delivery Documentation			Current year + 6 years	SECURE DISPOSAL
Debtors' Records		Limitation Act 1980	Current year + 6 years	SECURE DISPOSAL
School Fund – Cheque books			Current year + 3 years	SECURE DISPOSAL
School Fund – Paying in books			Current year + 6 years then review	SECURE DISPOSAL
School Fund – Ledger			Current year + 6 years then review	SECURE DISPOSAL
School Fund – Invoices			Current year + 6 years then review	SECURE DISPOSAL
School Fund – Receipts			Current year + 6 years	SECURE DISPOSAL
School Fund – Bank statements			Current year + 6 years then review	SECURE DISPOSAL
School Fund – School Journey books			Current year + 6 years then review	SECURE DISPOSAL
Student grant applications			Current year + 3 years	SECURE DISPOSAL
Petty cash books		Financial Regulations	Current year + 6 years	SECURE DISPOSAL

Property				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
Title Deeds			Permanent	These should follow the property unless the property has been registered at the Land Registry
Plans			Permanent	Retain in school whilst operational
Maintenance and contractors		Financial Regulations	Current year + 6 years	SECURE DISPOSAL
Leases			Expiry of lease + 6 years	SECURE DISPOSAL
Lettings			Current year + 3 years	SECURE DISPOSAL
Burglary, theft and vandalism report forms			Current year + 6 years	SECURE DISPOSAL
Maintenance log books			Current year + 6 years	SECURE DISPOSAL
Contractors' Reports			Current year + 6 years	SECURE DISPOSAL

Department for Education				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
HMI reports			These do not need to be kept any longer	
OFSTED reports and papers			Replace former report with any new inspection report	Review to see whether a further retention period is required
ISI reports and paper			Replace former report with any new inspection report	Review to see whether a further retention period is required
Returns			Current year + 6 years	SECURE DISPOSAL
Circulars from DFE			Whilst operationally required	Review to see whether a further retention period is required

School Meals				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
Lunch Register			Current year + 3 years	SHRED
School Meals Summary Sheets			Current year + 3 years	SHRED

APPENDIX 3 – Data Breach Report Form

This form is for staff to complete, following the initial report of an information incident. It should not take more than 15 minutes to complete.

Please provide as much information as possible. If you do not know the answer or you are waiting on the completion of further enquiries please state this and indicate when this information may be available. In addition to completing the form below, please provide any other supporting information that maybe relevant.

In the wake of an information incident, swift containment and recovery of the situation is vital. Where information has been sent to the wrong recipient immediate efforts should be made to retrieve the information. Every effort should be taken to minimise the potential impact on affected individuals and the Council, and details of the steps taken to achieve this should be included in this form.

Contact Details

Please provide your contact details should we require further information concerning the incident (Name and job title, email address and contact telephone number)	

Details of the information incident

Please describe the incident in as much detail as possible.	
When did the incident happen? (time and date)	
How did the incident happen?	
If there has been a delay in reporting the incident please explain your reason(s) for this.	
What measures and operational controls were in place to prevent and/or detect an incident of this nature occurring?	
Please provide the name and job title of the individual who was responsible for the breach.	

Personal data placed at risk

What, if any, personal data has been placed at risk? Please specify if any financial or personal sensitive data has been affected and provide details of the extent.	
How many individuals does the data relate to?	
Have the affected individuals been made aware that an incident has occurred?	
What are the potential risks, consequences and adverse effects on those individuals?	

Have any of the affected individuals complained about the incident and if so, what action has been taken?	

Containment and Recovery

Has any action been taken to minimise/mitigate the effect on the affected individual(s)? If so, please provide details.	
Has the information placed at risk now been recovered? If so, please provide details of how and when this occurred.	
Have any steps been taken to prevent a recurrence of this incident? If so, please provide details.	
Who have you informed about the incident, both internal and external? For example, in the event of theft, have the Police been informed and do you have a crime number?	

Training and guidance

Please confirm that all employees involved with the incident have successfully completed the Council's mandatory GDPR training?	
Has any additional Information Governance training been provided? If so, please provide details.	
Has any specific detailed operational guidance been developed and provided to staff on handling information, including the use of Council IT equipment? If so, please provide details.	

Previous information incidents

Have you (your department/team) reported any previous information incidents in the last year?	
If the answer is yes, please provide brief details.	

Investigation

Have you asked any questions to determine the circumstances leading to the loss of information? If so, please provide details.	

What, if any actions have been taken to preserve evidence and/or create an audit trail relating to the information incident?	
What, if any, remedial actions have been taken since the information incident occurred to prevent any recurrence?	
Where remedial actions have been identified what timescales have been agreed for their implementation? Please provide details.	

Sending this form

Send your completed form and any related attachments within one day of the date of the incident to **ciu@iow.gov.uk** with 'Information Incident Report Form' in the subject field.

What happens next?

When we receive this form, we will contact you to provide:

- An incident reference number; and
- Information about our next steps

If you need any help in completing this form, please contact the Corporate Information Unit, **ciu@iow.gov.uk** or telephone extensions 6329, 6387, 6330 or 6328.

Corporate Information Unit Use Only:	
Reference Number	
Severity / Impact Rating	

APPENDIX 4 - The following process should be followed to categorise a DPI

Step 1: Establish the scale of the incident. If this is not known it will be necessary to estimate the maximum potential scale point.

Baseline Scale Point	
0	Information about less than 10 individuals
1	Information about 11-50 individuals
2	Information about 51-100 individuals
3	Information about 101-300 individuals
4	Information about 301 – 500 individuals
5	Information about 501 – 1,000 individuals
6	Information about 1,001 – 5,000 individuals
7	Information about 5,001 – 10,000 individuals
8	Information about 10,001 +

Step 2: Sensitivity Factors modify baseline scale point

Low: For each of the following factors reduce the baseline score by 1 scale point	
-1 for each	No sensitive personal data or other sensitive information at risk
	Limited demographic data at risk e.g. address not included, name
	Security controls/difficulty to access data partially mitigates risk
	Confirmed that there is no link between the data subject and
	Sent to wrong recipient but not received or returned unopened

Medium: The following factors have no effect on baseline score	
0	Basic demographic data at risk e.g. equivalent to telephone directory
	Limited sensitive personal data at risk
	Unconfirmed or possible link between data subject and recipient

High: For each of the following factors increase the baseline score by 1 scale point	
	Detailed or multiple persons sensitive personal information at risk

+1 for each	Particularly sensitive information at risk
	One or more previous incidents of a similar type in past 12 months
	Failure to securely encrypt mobile technology or other obvious
	Newsworthy aspects or media interest
	A complaint has been made to the Information Commissioner
	Individuals affected are likely to suffer significant distress or
	Individuals affected have been placed at risk of physical harm
	Individuals affected may suffer significant detriment e.g. financial
	Incident has incurred or risked incurring a clinical untoward incident
	Confirmed link between data subject and recipient

Final Score	Level of DPI
0	Level 0 DPI
1 or 2	Level 1 DPI
3 - 5	Level 2 DPI
6 - 8	Level 3 DPI

APPENDIX 5 - Examples of personal data breaches and who to notify

Example	Notify the ICO?	Notify the data subject?	Notes/ recommendations
(i) A controller stored a backup of an archive of personal data encrypted on a USB key. The key is stolen during a break-in.	No	No	As long as the data are encrypted with a state of the art algorithm, backups of the data exist the unique key is not compromised, and the data can be restored in good time, this may not be a reportable breach. However if it is later compromised, notification is required.
(ii) A brief power outage lasting several minutes at a controller's call centre meaning customers are unable to call the controller and access their records.	No	No	This is not a notifiable breach, but still a recordable incident under Article 33(5). Appropriate records should be maintained by the controller.
(iii) An individual phones a bank's call centre to report a data breach. The individual has received a monthly statement for someone else. The controller undertakes a short investigation (i.e. completed within 24 hours) and establishes with a reasonable confidence that a	Yes	Only the individuals affected are notified if there is high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the supervisory authority must be made and the controller takes the additional step of notifying other individuals if there is high risk to them.

personal data breach has occurred and whether it has a systemic flaw that may mean other individuals are or might be affected.			
(iv) Medical records in a hospital are unavailable for the period of 30 hours due to a cyber-attack.	Yes, the hospital is obliged to notify as high-risk to patient's well-being and privacy may occur.	Yes, report to the affected individuals.	
(v) Personal data of a large number of students are mistakenly sent to the wrong mailing list with 1000+ recipients.	Yes, report to supervisory authority.	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	
(vi) A direct marketing e-mail is sent to recipients in the "to:" or "cc:" fields, thereby enabling each recipient to see the email address of other recipients.	Yes, notifying the supervisory authority may be obligatory if a large number of individuals are affected, if sensitive data are revealed (e.g. a mailing list of a psychotherapist) or if other factors present high risks (e.g. the mail contains the initial passwords).	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.

Appendix 6

Transfer of Pupil Files

I am enclosing the following files:
(please tick)

WWW.LANESENDPRIMARY.CO.UK

- ☐ **Office**
- ☐ **Classroom**
- ☐ **Additional Needs**
- ☐ **Early Help including CAF**
- ☐ **Child Protection / CIN**
- ☐ **CTF has been actioned**

For:

Pupil Name: _____ **Date of Birth:** _____

Year Group: _____

On the occasion of postal transfer, please return a copy of this form to the school office, marked for the attention of Caroline Sice.

Kindest Regards

Delivered by: _____
(Sign & print)

Date: _____

Received by: _____
(Sign & print)

School: _____

Date: _____

LANESEND PRIMARY SCHOOL
LOVE LANE, COWES
ISLE OF WIGHT PO31 7ES
TEL & FAX: 01983 293 233
E: ADMIN@LANESENDPRI.IOW.SCH.UK
HEADTEACHER: CAROLINE SICE