THE DINGLE PRIMARY SCHOOL
Data Protection Policy
(GDPR Regulations)

Updated: March 2025
Review Date: March 2026*
(*earlier if amendments to legislation)

The Dingle Primary School
The Dingle
Haslington
Crewe
CW1 5SD

Contents

1. AIMS

The Dingle Primary School aims to ensure that all data collected about staff, pupils, parents and visitors is collected, stored and processed in accordance with the Data Protection Act 1998 and the General Data Protection Regulations (GDPR) 2018.

This policy applies to all data, regardless of whether it is in paper or electronic format.

The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, details of which can be found in our Privacy Notices **(available on our school website www.dingle.cheshire.sch.uk)**

This policy has been developed to ensure all staff and governors are aware of their responsibilities and outlines how the school complies with the core principles of GDPR.

2. LEGAL FRAMEWORK AND GUIDANCE

This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation 12 steps to take now'

This policy will be implemented in conjunction with the following other school documents:

- Photograph Consent
- Acceptable use Policy
- E-safety Policy
- Freedom of Information Publication Scheme
- Retention Schedule

3. DEFINITIONS

TERM	DEFINITION
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Sensitive Personal data	Data such as: • Contact details • Racial or ethnic origin • Political opinions • Religious beliefs, or beliefs of a similar nature

	• Where a person is a member of a trade union • Physical and mental health • Sexual orientation • Whether a person has committed, or is alleged to have committed, an offence • Criminal convictions
Processing	Obtaining, recording or holding data
Data subject	The person whose personal data is held or processed
Data controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller

4. THE DATA PROTECTION OFFICER (DPO)

The Dingle Primary School processes personal information relating to pupils, staff and visitors, and is therefore, the Data Controller. Our school delegates the responsibility of data control to the Data Protection Officer 'DPO' who can be contact by emailing DPO@dingle.cheshire.sch.uk.

The school is registered as a Data Controller with the Information Commissioner's Office under reference number Z6204085. This registration is updated annually in May.

The DPO has the necessary experience and knowledge of data protection law, particularly in relation to schools and their role is to:

- Inform and advise the school and its employees about their obligations to comply with the GDPR and other Data Protection laws.
- Monitor the school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.
- Report to the highest level of management at the school, which is the Headteacher.
- Operate independently and will not be dismissed or penalised for performing their task.
- Be provided with sufficient resources to enable them to meet their GDPR obligations.

5. DATA PROTECTION PRINCIPLES

In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- Accurate and up-to-date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- 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.

6. GDPRis PLATFORM

The Dingle Primary School uses "The GDPRis Platform" as a software tool to hold all GDPR data in one secure area. The GDPRis platform ensures that all data being processed is measurable and compliant with the GDPR principles.

The Dingle Primary School has comprehensive, clear and transparent Privacy Notices and internal records of processing activities that include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Data mapping
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third parties, including documentation of the transfer mechanism safeguards in place

The school Privacy Notice can be found on our website www.dingle.cheshire.sch.uk.

The school ensures that it meets the principles of data protection by:

- Data minimisation
- Pseudonymisation
- Transparency
- Allowing individuals to monitor processing
- Continuously creating and improving security features

7. ROLES AND RESPONSIBILITIES

The Governing Body has overall responsibility for data protection. The Governing Body has named Caroline Lambert as the Governor responsible for ensuring that the school complies with its obligations under GDPR. The Governing Body will carry out their statutory duties in relation to GDPR by undertaking regular monitoring of the GDPRis Platform.

Day-to-day responsibility rests with the Headteacher, or the School Business Manager in the absence of the Headteacher. The Headteacher will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this Policy. They are also asked to comply with the GDPR Confidentiality Security Reminders: Non-Negotiables shown at **Appendix 1.**

8. LAWFUL PROCESSING

The legal basis for processing data will be identified and documented prior to data being processed.

Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained
- Processing is necessary for:
  - Compliance with a legal obligation.
  - The performance of a task carried out in the public interest
  - For the performance of a contract with the data subject or to take steps to enter into a contract
  - Protecting the vital interests of a data subject or another person
  - For the purposes of legitimate interests

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject
- Processing carried out by a not-for-profit body, provided there is no disclosure to a third party without consent
- Processing relates to personal data manifestly made public by the data subject
- Processing is necessary for:
  - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
  - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
  - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
  - Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
  - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
  - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
  - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

9. CONSENT

Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes and will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes. Where consent is given, a record will be kept documenting how and when consent was given.

The school will ensure that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

Consent previously accepted under the Data Protection Act must be reviewed to ensure it meets the standards of the GDPR.

Consent can be withdrawn by the individual at any time.

10. THE RIGHT TO BE INFORMED

The Privacy Notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge and will include:

- The identity and contact details of the controller (and where applicable, the controller's representative) and the DPO
- The purpose of, and the legal basis for, processing the data
- The legitimate interests of the controller or third party
- Any recipient or categories of recipients of the personal data
- Details of transfers to third countries and the safeguards in place
- The retention period of criteria used to determine the retention period
- The existence of the data subject's rights, including the right to:
  - Withdraw consent at any time.
  - Lodge a complaint with the Information Commissioner's Office (ICO).
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

11. THE RIGHT OF ACCESS

Individuals have the right to obtain confirmation that their data is being processed and have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

Upon receiving a SAR the school will verify the identity of the person making the request before any information is supplied. Copies of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within one month of receipt.

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

12. THE RIGHT TO RECTIFICATION

Individuals are entitled to have any inaccurate or incomplete personal data rectified. Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.

Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual, and will inform them of their right to complain to the ICO.

13. THE RIGHT TO ERASURE

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. The right to erasure may occur in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

14. THE RIGHT TO RESTRICT PROCESSING

Individuals have the right to block or suppress the school's processing of personal data. In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

The school may restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
- Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

The school will inform individuals when a restriction on processing has been lifted.

15. THE RIGHT TO DATA PORTABILITY

Individuals have the right to obtain and reuse their personal data for their own purposes across different services. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability. The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

Personal data will be provided in a structured, commonly used and machine-readable form. The school will provide the information free of charge. Where feasible, data will be transmitted directly to another organisation at the request of the individual.

The school is not required to adopt or maintain processing systems which are technically compatible with other organisations. In the event that the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual.

The school will respond to any requests for portability within one month.

Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request. Where no action is being taken in response to a request, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the ICO and to a judicial remedy.

16. THE RIGHT TO OBJECT

The school will inform individuals of their right to object at the first point of communication, and this information will be outlined in the Privacy Notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- The school will stop processing personal data for direct marketing purposes as soon as an objection is received.

- The school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.

Where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above, but is carried out online, the school will offer a method for individuals to object online.

17. AUTOMATED DECISION MAKING AND PROFILING

Individuals have the right not to be subject to a decision when:

- It is based on automated processing, e.g. profiling.
- It produces a legal effect or a similarly significant effect on the individual.

The school will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it. When automatically processing personal data for profiling purposes, the school will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- The school has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

18. PRIVACY BY DESIGN AND PRIVACY IMPACT ASSESSMENTS

The school will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into processing activities.

Data Protection Impact Assessments (DPIAs) will be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

A DPIA will be used for more than one project, where necessary.

The school will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

Where a DPIA indicates high risk data processing, the school will consult the Information Commissioner's Office (ICO) to seek its opinion as to whether the processing operation complies with the GDPR.

19. DATA BREACHES

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The Headteacher will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their induction and through staff briefings.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the ICO will be informed.

All notifiable breaches will be reported to the ICO within 72 hours of the school becoming aware of it.

The risk of the breach having a detrimental effect on the individual, and the need to notify the ICO, will be assessed on a case-by-case basis.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly.

A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the ICO.

In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Effective and robust breach detection, investigation and internal reporting procedures are in place at the school, which facilitate decision-making in relation to whether the ICO or the public need to be notified. Staff are aware that all data breaches need to be recorded on the GPDRis Platform.

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

20. DATA SECURITY

Staff must ensure that the following data security measures are in place:

- Confidential paper records are kept in a locked filing cabinet, drawer or safe, with restricted access. Confidential paper records are never left unattended or in clear view anywhere with general access.
- Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.
- Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.
- All Memory Sticks are fully encrypted.
- All electronic devices are password-protected to protect the information on the device in case of theft and where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- Staff and governors will not use their personal laptops or computers for school purposes unless they are personally password-protected and fully encrypted.
- All staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.
- Emails containing sensitive or confidential information are sent via the 'Egress' system and are password-protected.
- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

Before sharing data, all staff will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in the school's Privacy Notice.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.

The physical security of the school's buildings and storage systems, and access to them, is reviewed on a regular basis.

The Dingle Primary School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

The School Business Manager (SBM) is responsible for ensuring that continuity and recovery measures are in place to ensure the security of protected data.

Staff have received a copy of GDPR Confidentiality Reminder Sheet as shown at Appendix 1.

21. PUBLICATION OF INFORMATION

The Dingle Primary School has a Freedom of Information Publication Scheme on our website outlining classes of information that are routinely available, including:

- School Prospectus - information published in the school prospectus
- Governors' Documents ("in accordance with the Freedom of Information Act")
- Pupils & Curriculum - information about policies that relate to pupils and the school curriculum. School Policies and Procedures regarding Financial information.
- Classes of information specified in the publication scheme are made available quickly and easily on request.

The Dingle Primary School will not publish any personal information, including photos, on its website without the permission of the child's parent or guardian.

When uploading information to the school website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

22. PHOTOGRAPHY

The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

The school always indicates its intentions for taking photographs of pupils and will retrieve permission before publishing them.

If the school wishes to use images/video footage of pupils in a publication, such as the school website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

23. DATA RETENTION

The Dingle Primary School will not keep data longer than is necessary, it will also:

- Delete unrequired data as soon as practicable.
- Shred all unrequired paper documents
- Delete, clean or destroy all electronic memories
- Handle DBS data in line with data protection legislation
- Never photocopy DBS documentation; Any third parties who access DBS information will be made aware of the Data Protection legislation, as well as their responsibilities as a data handler.

For further information, please refer to the Retention Schedule.

24. WHAT GDPR MEANS AT THE DINGLE PRIMARY SCHOOL

This Policy has given details of the legal framework for GDPR but what does this mean for parents, pupils and staff at The Dingle Primary School?

Pupils and Parents

We hold personal data about pupils to support teaching and learning, to provide pastoral care and to assess how the school is performing. We may also receive data about pupils from other organisations including, but not limited to, other schools, local authorities and the Department for Education.

How we use and why we collect pupil information can be found on the Privacy Notice (which can be found on our website www.dingle.cheshire.sch.uk)

Staff

We hold and process personal data relating to those we employ to work at, or otherwise engage to work at, our school. This is for employment purposes to assist in the running of the school and/or to enable individuals to be paid.

25. SUBJECT ACCESS REQUESTS

Under the Data Protection Act 1998, pupils and staff have a right to request access to information the school holds about them. This is known as a Subject Access Request or SAR.

Subject access requests must be submitted in writing, either by letter, email. Requests should include:

- The pupil/ staff name
- A correspondence address
- A contact number and email address
- Details about the information requested

The school will not reveal the following information in response to subject access requests:

- Information that might cause serious harm to the physical or mental health of the pupil or another individual
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child

Subject Access Requests for all or part of the pupil's educational record will be provided within 15 school days.

If a subject access request does not relate to the educational record, we will respond within 40 calendar days.

26. PARENTAL REQUESTS TO SEE THE EDUCATIONAL RECORD

Parents have the right to request access to their child's educational record, free of charge, within 15 school days of a request.

If parents ask for copies of information, they will be required to pay the cost of making the copies.

Parents of pupils at this school do not have an automatic right to access their child's educational record. The school will decide on a case-by-case basis whether to grant such requests, and we will bear in mind guidance issued from time to time from the Information Commissioner's Office.

27. TRAINING

Our staff and governors are provided with Data Protection and GDPR training as part of their induction process and through CPD, where changes to legislation or the school's processes make it necessary.

28. MONITORING ARRANGEMENTS

The Headteacher monitors and ensures that school staff comply with this policy by checking that staff declare any security breaches on the GDPRis Platform and that they comply with the GDPR Confidentiality Security Reminders Non-Negotiables as shown at **Appendix 1.**

This document will be reviewed **every 3 years** or earlier if legislation changes.

The Governing Body is responsible for ensuring that the school complies with its obligations under GDPR and that there is a Governor nominated to undertake this role through Governor monitoring.

Confirmation the *GDPR Policy* in respect of The Dingle Primary School has been discussed and adopted by the Governing Body

Signed……. Dated……..

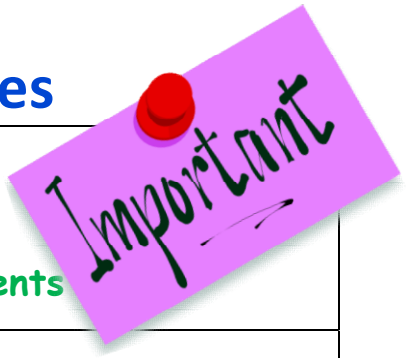
Headteacher

Signed…… *Dated……*

R Smith - Chair of Governors

GDPR CONFIDENTIALITY

SECURITY REMINDERS: Non-negotiables



	Ensure your DESK IS CLEAR AND TIDY at the end of the day		Ensure you LOCK UP ALL confidential documents
	nsure you take all RINTED DOCUMENTS rom the printer		Ensure the PRINTER IS PASSWORD Protected NEVER share login details
	Always LOCK YOUR SCREEN When away from your PC		Never leave IMPORTANT DOCUMENTS At meetings/in vehicles etc.
	Never keep IMPORTANT DATA OR DOCS In your pigeon hole		Don't erase, destroy SHRED ALL DATA Don't stockpile information
	Always change PASSWORDS frequently NEVER share login details		Only use ENCRYPTED USB ALL devices MUST BE encrypted
	REPORT ALL DATA BREACHES TO THE HEADTEACHER & DPO IMMEDIATELY **School has 72 hours within which is report a data breach to the ICO**		