

Davenham Church of England Primary School

“Working Together, Playing Together, Serving God and Serving Others”

“...encourage one another and build each other up...”

POLICY FOR DATA PROTECTION

1. Legal framework

1.1. 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

1.2. This policy will also have regard to the following guidance:

- Information Commissioner’s Office (2017) ‘Overview of the General Data Protection Regulation (GDPR)’
- Information Commissioner’s Office (2017) ‘Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now’
- All Article 29 Working Party Guidance on the implementation of GDPR
- Department of Education ‘Data Protection: a toolkit for schools’
- IRMS Information Management Toolkit for Schools.

1.3. This policy will be implemented in conjunction with the following other school policies:

- IT Acceptable Use Policy
- Freedom of Information Policy
- Social Media Policy

2. Applicable data

For the purpose of this policy:

2.1. Personal data refers to information that relates to an identified or identifiable, living individual (Data Subject), including an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.2. Sensitive personal data is defined in the GDPR as 'special categories of personal data', which includes the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation .

2.3 Processing Data is referred to throughout the GDPR and data protection legislation. This means any use of the personal information. This includes collecting, disclosing, destroying, archiving and organising.

2.4 Data Subject is the person who the personal data is about. For example, the children named on a class register at a school are all data subjects of that register.

2.5 Data Controller is usually an organisation who dictates the reason and purpose for how data is processed. The school itself is a Data Controller as it chooses how it collects, uses and shares its own data.

2.6 The Information Commissioner's Office (ICO) is the regulator for Data Protection and Privacy law in the UK. They have the power to enforce on organisations for breaches of the Data Protection Act or the GDPR. This means they can issue: -

- An Undertaking which commits an organisation to improving their Data Protection practices.
- An Enforcement Notice ordering that an organisation does something specific e.g. train all staff to a high standard.
- A Monetary Penalty for serious and significant breaches. Under the Data Protection Act, this can be anything up to £500,000. Under the General Data Protection Regulation this can be up to €20 Million or 4% of a company's global turnover.

2.3 This policy applies to both automated personal data and to manual filing systems.

3. Principles

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

1. Processed Fairly, Lawfully and Transparently
2. Processed for a Specified and Legitimate Purpose
3. Adequate, Relevant and limited to what is relevant
4. Accurate and up to date
5. Kept no longer than necessary

6. Stored securely using technical and organisational measures

3.2. The GDPR also requires that “the controller (the school) shall be responsible for, and able to demonstrate, compliance with the principles”.

4. Accountability

4.1. Davenham C of E Primary School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR. This can take a variety of forms. Examples of technical and organisational measures can be found below.

Technical Measures

- Firewalls
- Anti-virus software
- Encryption
- Secure emails
- VPNs (Virtual Private Networks)

Organisational Measures

- Policies and Procedures in place to help staff understand their duties under data protection
- Training
- A more knowledgeable and open culture towards Data Protection

4.2. Davenham C of E Primary School will provide comprehensive, clear and transparent privacy notices.

4.3. Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data.

4.4. In line with best practice, we shall create a record of processing activities will include as a minimum the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures

4.5. Davenham C of E Primary School will implement measures that meet the principles of data protection, continuously creating and improving security features.

4.6. Davenham C of E Primary School will produce Data protection Impact Assessments where the processing of personal data is likely to result in a high risk to the rights of the individual, where a major project requires the processing of personal data or before the introduction of new technology or a significant change to the way processing is performed.

5. Data protection officer (DPO)

5.1. Davenham C of E Primary School has appointed a DPO in order 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.

5.2. The role of DPO will be carried out by an experienced and qualified member of staff as designated by Cheshire West and Chester Council.

5.3. Davenham C of E Primary School will make freely available the contact details for their appointed DPO:

Martin Waters | Schools Data Protection Officer

Data Protection Compliance | Governance

SchoolDPO Support Service 2020/21

Email: SchoolDPO@cheshirewestandchester.gov.uk

Mobile: 07990786929

Office: 01244 9 72245

Cheshire West and Chester Council

Postal Address: 3rd Floor, Civic Way, 4 Civic Way, Ellesmere Port, CH65 0BE

Visit: cheshirewestandchester.gov.uk

Our ICO registration no is Z6619057 which is renewed every year on 17th December.

5.4. The DPO will operate independently, their role being to:

- advise Davenham C of E Primary School and its employees about the obligations to comply with GDPR and other data protection requirements – for example this could be to assist in implementing a new CCTV system or to respond to questions or complaints about information rights.
- monitor your school's compliance with GDPR, advising on internal data protection activities such as training for staff, the need for data protection impact assessments and conducting internal audits.

- act as the first point of contact with the Information Commissioner's Office and for individuals whose data you process.

5.5. Where advice and guidance offered by the DPO is rejected by the school, this will be independently recorded.

5.6 Advice offered by the DPO will only be declined at the direction of the Head and/or Governing body and will be provided to the DPO in writing.

6. Lawful processing

6.1. The legal basis for processing data will be identified and documented prior to data being processed. Davenham C of E Primary School will make it clear, at all times, the basis on which personal data is processed.

6.2. Davenham C of E Primary School will ensure that, where it processes personal data it will be lawfully processed under one of the following conditions:

- Compliance with a legal obligation.
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- 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 pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

6.3. In addition, Davenham C of E Primary School will ensure that the processing of sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- 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 here the data subject is physically or legally incapable of giving consent.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and 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 the establishment, exercise or defence of legal claims

- Processing is necessary for reasons of substantial public interest, on the basis of Union or Member state law, with full regard for the rights and interests of the data subject.
- Processing is necessary for the purposes of preventive or occupational medicine, for example, the assessment of the working capacity of the employee
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

7. Consent

7.1. Where there is no other legal basis for the processing of data Davenham C of E Primary School may rely on the consent of individuals, both parents and pupils, in seeking consent.

7.1. Where used, consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

7.2. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

7.3. Where consent is given, a record will be kept documenting how and when consent was given.

7.4. Consent previously accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

7.5. Consent can be withdrawn by the individual at any time.

7.6. The consent of parents will be sought prior to the processing of a child's data under the age of 12 except where the processing is related to preventative or counselling services offered directly to a child.

8. The right to be informed

8.1. The privacy notice supplied to individuals in regard to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

8.2. If services are offered directly to a child, Davenham C of E Primary School will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

8.3. In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- 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.
- Any 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 a supervisory authority.

8.4. 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 and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

9. The right of access

9.1. Individuals have the right to obtain confirmation that their data is being processed.

9.2. Individuals 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. A form for requesting information is available on the Website or from the school office.

9.3. Davenham C of E Primary School will verify the identity of the person making the request before any information is supplied as well as confirming the subject of the request and the right to make such a request (see 9.12. and 9.13)

9.4. A copy of the information will be supplied to the individual free of charge; however, Davenham C of E Primary School may impose a 'reasonable fee' to comply with requests for further copies of the same information.

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

9.6. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee may be charged.

9.7. All fees will be based on the administrative cost of providing the information.

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

9.9. 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.

9.10. Where a request is manifestly unfounded or excessive, Davenham C of E Primary 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 supervisory authority and to a judicial remedy, within one month of the refusal.

9.11. In the event that a large quantity of information is being processed about an individual, Davenham C of E Primary School may ask the individual to specify the information the request is in relation to.

9.12. A parent or guardian does not have an automatic right to information held about their child. The right belongs to the child and the parent(s) acts on their behalf, where they have parental responsibility for the child. In England the age at which a child reaches sufficient maturity to exercise their own right to access their information is normally 12, but this may vary amongst individuals. Once a child reaches sufficient maturity, the parent may only act with their child's consent.

9.13. Where a child is over 12 and a request is made on their behalf, Davenham C of E Primary School may contact them separately to seek their signed consent for someone to access their records on their behalf. When deciding whether information about a child can be released, consideration will be given to the best interests of the child.

9.14. Davenham C of E Primary School will clearly communicate and promote the process for the submission of Subject Access Requests and the exercising of other individual rights as defined under the GDPR during holiday periods, stating clearly how Davenham C of E Primary School will handle these requests and how this may impact on any time scales.

10. The right to rectification

10.1. Individuals are entitled to have any inaccurate or incomplete personal data rectified.

10.2. Where appropriate, Davenham C of E Primary School will inform the individual about the third parties that the data has been disclosed to.

10.3. Where the personal data in question has been disclosed to third parties, Davenham C of E Primary School will inform them of the rectification where possible.

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

10.5. Where no action is being taken in response to a request for rectification, Davenham C of E Primary School will explain the reason for this to the individual and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

11. The right to erasure

11.1. Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

11.2. The right to erasure is not absolute. Individuals have the right to erasure 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

11.3 Davenham C of E Primary 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

11.4. As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

11.5. 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.

11.6. Where personal data has been made public within an online environment, Davenham C of E Primary School will inform other organisations who process the

personal data to erase links to and copies of the personal data in question where possible.

12. The right to restrict processing

12.1. Individuals have the right to block or suppress the school's processing of personal data.

12.2. In the event that processing is restricted, Davenham C of E Primary 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.

12.3. Davenham C of E Primary School will 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 Davenham C of E Primary School has verified the accuracy of the data
- Where an individual has objected to the processing and Davenham C of E Primary 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 Davenham C of E Primary School no longer needs the personal data, but the individual requires the data to establish, exercise or defend a legal claim

12.4. If the personal data in question has been disclosed to third parties, Davenham C of E Primary 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.

12.5. Davenham C of E Primary School will inform individuals when a restriction on processing has been lifted.

13. The right to data portability

13.1. Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

13.2. 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.

13.3. The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a Davenham C of E Primary School
- 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

13.4. Personal data will be provided in a structured, commonly used and machine-readable form.

13.5. Davenham C of E Primary School will provide the information free of charge.

13.6. Where feasible, data will be transmitted directly to another organisation at the request of the individual.

13.7. Davenham C of E Primary School is not obligated to adopt or maintain processing systems which are technically compatible with other organisations.

13.8. In the event that the personal data concerns more than one individual, Davenham C of E Primary School will consider whether providing the information would prejudice the rights of any other individual.

13.9. Davenham C of E Primary School will respond to any requests for portability within one month.

13.10. 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.

13.11. Where no action is being taken in response to a request, Davenham C of E Primary 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 supervisory authority and to a judicial remedy.

14. The right to object

14.1. Davenham C of E Primary 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.

14.2. 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 undertaken by or on behalf of the school
- Processing for purposes of scientific or historical research and statistics.

14.3. 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.

- Davenham C of E Primary School will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where Davenham C of E Primary School can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

14.4. Where personal data is processed for direct marketing purposes:

- Davenham C of E Primary School will stop processing personal data for direct marketing purposes as soon as an objection is received.
- Davenham C of E Primary School cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

14.5. 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, Davenham C of E Primary School is not required to comply with an objection to the processing of the data.

14.6. Where the processing activity is outlined above, but is carried out online, Davenham C of E Primary School will offer a method for individuals to object online.

15. Privacy by design and Data Protection Impact Assessments

15.1. Davenham C of E Primary School will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how Davenham C of E Primary School has considered and integrated data protection into processing activities.

15.2. 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.

15.3. DPIAs will allow Davenham C of E Primary 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.

15.4. A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

15.5. A DPIA may be used for more than one project, where necessary and where the aims and conditions of the project are the same.

15.6. Davenham C of E Primary 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

15.7. Where a DPIA indicates high risk data processing, Davenham C of E Primary School will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

16. Data Processors

16.1 Davenham C of E Primary School will ensure that whenever it employs or utilises a data processor a written contract will be in place.

16.2. Any contract will include, as a minimum, specific terms under which processing is allowed and will document:

- only act on the written instructions of the controller;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the controller and under a written contract;
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract; and
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

16.3. Where appropriate, and if and when supplied by the Information Commissioner's Office, standard clauses may be supplemented.

16.4. Any contract will clearly identify the responsibilities and liabilities of data processors in relation to:

- not to use a sub-processor without the prior written authorisation of the data controller;

- to co-operate with supervisory authorities (such as the ICO);
- to ensure the security of its processing;
- to keep records of processing activities;
- to notify any personal data breaches to the data controller;
- to employ a data protection officer; and
- to appoint (in writing) a representative within the European Union if needed.

16.5. Where a processor fails in these obligations or acts outside of the direct instructions of the school, appropriate action will be taken.

17. Data breaches

17.1. 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.

17.2. Davenham C of E Primary School will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their continuous development training.

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

17.4. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of Davenham C of E Primary School becoming aware of it by the school's Data Protection Officer.

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

17.6. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, Davenham C of E Primary School will notify those concerned directly.

17.7. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

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

17.9. 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 relevant supervisory authority or the public need to be notified.

17.10. 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

17.11. Failure to report a breach when required to do so will be a breach of school policy and an additional breach of the GDPR.

18. Data security

18.1. Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

18.2. Confidential paper records will not be left unattended or in clear view anywhere with general access.

18.3. 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.

18.4. Where data is saved on removable storage or a portable device, the device will be kept safe when not in use.

18.5. Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

18.6. All electronic devices are password-protected to protect the information on the device in case of theft.

18.7. Where possible, Davenham C of E Primary School enables electronic devices to allow the remote blocking or deletion of data in case of theft.

18.8. Staff and governors will not use their personal laptops or computers for school purposes.

18.9. All necessary members of staff are provided with their own secure login and password

18.10. Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

18.11. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

18.12. When sending confidential information by fax, staff will always check that the recipient is correct before sending.

18.13. 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 Davenham C of E Primary School premises accepts full responsibility for the security of the data.

18.14. Before sharing data, all staff members 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 a privacy notice.

18.15. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of Davenham C of E Primary School containing sensitive information are supervised at all times.

18.16. The physical security of the school's buildings and storage systems, and access to them, is reviewed regularly and at least every line in line with the review of this policy. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

18.17. Any unauthorised disclosure or personal or sensitive information may result in disciplinary action.

19. Publication of information

19.1. Davenham C of E Primary School will not publish any personal information, including photos, on its website, in social media or in any promotional or marketing publication without the permission of the affected individual.

19.4. When uploading information to Davenham C of E Primary School website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

20. Data retention

20.1. Data will not be kept for longer than is necessary in line with the schools Record Management Policy.

21.2. Unrequired data will be deleted as soon as practicable.

21.3. Some educational records relating to former pupils or employees of Davenham C of E Primary School may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

21.4. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

21. DBS data

21.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

21.2. Data provided by the DBS will never be duplicated.

21.3. 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.

DATA BREACH PROCEEDURE

Davenham C of E Primary School holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. 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 procedure applies to all personal and sensitive data held by the school and all school staff, Governors, volunteers and contractors, referred to herein after as 'staff'.

It must be remembered that data does not necessarily have to be lost for it to be considered a breach, information may just be put at risk of loss for it to qualify.

In the case of serious breaches/incidents these must be reported to the Data Protection Officer as soon as they are identified. The DPO has a legal responsibility to assess the seriousness of any incident and report serious occurrences to the Information Commissioner's Office within 72 hours

Purpose

This breach procedure sets out the course of action to be followed by all staff at Davenham C of E Primary School if a data protection breach takes place.

1.0 Legal Context

Davenham C of E Primary School will comply with the requirements of Article 33 of the General Data Protection Regulations in relation to the Notification of a personal data breach to the supervisory authority

- 1.1. In the case of a personal data breach, the controller (the school) shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

- 1.2. The processor shall notify the controller (the school) without undue delay after becoming aware of a personal data breach.
- 1.3. The notification referred to in paragraph 1 shall at least:
 - (a) describe the 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) communicate 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.
- 1.4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
- 1.5. The controller (the school) shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

2.0 Types of Breach

2.1. Data protection breaches could be caused by a number of factors. A number of examples are shown below:

- Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Poor data destruction procedures;
- Human Error;
- Cyber-attack;
- Hacking.

3.0 Managing a Data Breach

In the event that the School identifies or is notified of a personal data breach, the following steps should followed:

- 3.1 The person who discovers/receives a report of a breach must inform the Head Teacher or the School Business Manager. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable. This should be done by completing the attached breach notification form.
- 3.2. The DPO (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.
- 3.3. The DPO (or SBM) must inform the Head/Chair of Governors as soon as possible if the breach is considered of a serious nature. As a registered Data Controller, it is the school's responsibility to take the appropriate action and conduct any investigation.
- 3.4. The DPO (or SBM) must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the School's legal support should be obtained.
- 3.5 The DPO (or SBM) will take the decision based on the severity of a breach and the likely effect on data subjects as to whether the ICO should be notified (this should occur within 72 hours of the incident being identified) and to whether the data subject should be notified.
- 3.5. The DPO (or SBM) must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:
 - a. Attempting to recover lost equipment.
 - b. Contacting the relevant Council Department, so that they are prepared for any potentially inappropriate enquiries for further information on the individual or individuals concerned. Consideration should be given to a global email to all school staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual, making the enquiry, back. Whatever the outcome of the call, it should be reported immediately to the Head Teacher/DPO (or nominated representative).
 - c. The use of back-ups to restore lost/damaged/stolen data.
 - e. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

- f. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately, and the relevant agencies and members of staff informed

INVESTIGATION PROCEDURE

1.0 Investigation

1.1 In most cases, the Data Protection Officer (DPO) or School Business Manager (SBM) will fully investigate the breach. The DPO (or SBM) should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data;
- Its sensitivity;
- What protections were in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach.

1.2 A clear record should be made of the nature of the breach and the actions taken to mitigate it.

1.3 The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office.

1.4 A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

2.0 Notification

2.1 Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place.

2.2 The DPO (or SBM) should decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be

notified within 72 hours of the breach. Every incident should be considered on a case by case basis.

2.3 When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the School is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the School's Complaints Procedure). The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach

3.0 Review and Evaluation

3.1 Once the initial aftermath of the breach is over, the DPO (or SBM) should fully review both the causes of the breach and the effectiveness of the response to it.

3.2 It should be reported to the next available Senior Management Team and Full Governors meeting for discussion.

3.3. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these rights.

3.4 If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources or Internal Audit for advice and guidance.

3.5 This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

4.0 Implementation

4.1 The DPO should ensure that staff are aware of the School's Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training.

4.2 If staff have any queries in relation to the School's Data Protection policy and associated procedures, they should discuss this with their line manager, DPO or the Head Teacher.

School Information Security Incident Reporting Form

Completed forms must be sent as soon as possible to *[School's Data Protection Lead/DPO]*

Provide as much information as you can, but do not delay sending in the form, incidents must be notified within 24 hours of identification.

GENERAL DETAILS	
Incident number:	<i>To be assigned by data protection lead</i>
Reported by:	<i>Named member of staff</i>
Date of incident:	<i>When did it occur?</i>
Date incident was identified:	<i>When was it identified</i>
Reported Date:	<i>Date DPO/DP Lead/Head Notified</i>
Location of incident:	<i>In school, offsite etc</i>
ABOUT THE INCIDENT – provide as much information as possible.	
Incident description. Please describe the incident in as much detail as possible	
How did the incident occur?	<i>Provide as much known information as possible</i>
When did the incident happen?	

	<i>If no accurate date can be identified, be approximate</i>
How was the incident identified?	<i>Was it discovered by the school, reported by a parent/3rd party?</i>
What personal data has been placed at risk?	<i>Details of information you believe may have been</i>
In what format was the information involved?	<i>Letter, email, USB pen etc.</i>
Was the data encrypted/appropriately secured?	<i>Was secure email used, was USB secure, if system access what controls were in place</i>
Dealing with the current incident	
Has the school taken any immediate action to minimise/mitigate the effect on the affected individuals?	<i>If so, provide details.</i>
How many individuals have been affected?	<i>Number of pupils, staff, parents etc. who may have been affected by information being put at risk</i>
Have any affected individuals complained to the school about the incident?	<i>Have they complained direct, have they referenced complaining to the ICO?</i>
What are the potential consequences and adverse effects on those individuals? (parents, pupils or staff)	<i>Don't just think worst case scenario, think of any consequences to individuals even if it is merely 'inconvenience'</i>

<p>Has the data subject been informed/is the data subject aware?</p>	<p><i>Have they already been told or are they likely to be aware e.g. parents talking to each other, was it reported in the press etc.?</i></p>	
<p>Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.</p>	<p><i>Can you verify the risk has been removed – the data recovered or destroyed, vulnerabilities addressed etc.</i></p>	
<p>Preventing a recurrence</p>		
<p>Has any action been taken to prevent recurrence?</p>	<p><i>What steps have been taken – policies, procedures, change in working practice, training etc.</i></p>	
<p>Are further actions planned? If so, what?</p>	<p><i>Have other actions been scheduled, e.g. an audit of processes, training etc.</i></p>	
<p>Who has the action been agreed by?</p>	<p><i>Has any action been signed off by Head, Governors, DPO etc.</i></p>	
<p>Individuals Involved</p>		
<p>Have the staff involved in the security incident done any Data Protection Training?</p>	<p><i>Document what training was carried out</i></p>	
<p>If so, what and when? (Please list)</p>	<p><i>Document when any/last training was carried out</i></p>	
<p>How long have those involved worked at the School?</p>	<p><i>Addresses whether training is required for new staff</i></p>	
<p>Are the staff involved: agency staff, new starters, part time staff, full time staff etc?</p>	<p><i>Addresses whether training is required for different levels of staff, governors etc.</i></p>	
<p>IMPACT ASSESSMENT QUESTIONS</p>		
<p>1.</p>	<p>Was any data lost or compromised in the incident?</p>	<p>Yes/No</p>

	E.g. Loss of an encrypted item should not actually have compromised any information	
2.	<p>Was personal data lost or compromised?</p> <p>This is data about living individuals such as pupil, staff, parents etc.</p>	Yes/No
3.	<p>If yes, was <u>sensitive</u> personal data compromised?</p> <p>This is data relating to health, ethnicity, sexual life, trade union membership, political or religious beliefs, philosophical beliefs, potential or actual criminal offences, genetic or biometric data.</p>	Yes/No
4.	<p>Does any of the information lost or compromised relate directly to a child/children?</p>	Yes/No
5.	<p>Was safeguarding, child protection or health data involved?</p>	Yes/No
6.	<p>What is the number of people whose data was affected by the incident?</p>	
7.	<p>Is the data breach <u>unlikely</u> to result in a <u>risk</u> to the individual/individuals?</p> <p>Physically, materially, or morally?</p> <p>Example - physical harm, fraud, reputation, financial loss, distress</p>	Yes/No
8.	<p>Did this incident involve information belonging to another organisation? e.g. NHS, Local Council, Police etc.</p>	Yes/ No
9.	<p>Did people affected by the incident give the information to the School in confidence? (i.e. with an expectation that it would be kept confidential)</p>	Yes/No
10.	<p>Is there a risk that the incident could lead to direct damage to any individual e.g. via identity theft/ fraud/impersonation?</p>	Yes/No

11.	Could the incident damage an individual's reputation, or cause hurt, distress, embarrassment or humiliation e.g. loss of medical records, disciplinary records etc.?	Yes/No
12.	Can the incident have a serious impact on the School's reputation?	Yes/No
13.	Has any similar incident happened before?	Yes/No
14.	Was the school aware such an incident was possible or likely to occur?	Yes/No

REVIEW: to be completed by Data Protection Lead/Data Protection Officer (where required)

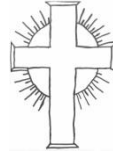
Incident Number:	
Classification:	<input type="checkbox"/> Breach <input type="checkbox"/> Incident <input type="checkbox"/> Offence
Principles identified as breached:	1) Lawful, fair and transparent
	2) Specific, explicit and legitimate purposes
	3) Adequate, relevant and limited to what is necessary for processing.
	4) Accurate and kept up to date
	5) Kept in a form that allows for the identification of data subjects only as long as necessary
	6) Processed in manner that ensures its security.
Is a full investigation required?	
Have data subjects been informed?	
Have key stakeholders (Parents, Governors, Local Authority etc) been informed?	

Have control weaknesses been highlighted and recommendations made?	
Has sufficient and appropriate action been taken?	
Does the incident need reporting to the DPO?	
Does the incident need reporting to the ICO?	
Has the Incident Log been updated?	
Further investigation undertaken by: -	
Notes: (Reasons for referral/non-referral to ICO)	

Sign off and Outcomes

Item	Name/Date	Notes
Measures to be implemented approved by:		<i>Responsibility for actions and required completion date – school DP Lead/Head</i>
DPO advice and recommendation provided:		<i>DPO advice in relation to mitigating risk, action to be taken</i>
Summary of DPO Advice:		
DPO Advice accepted or overruled by:		<i>If overruled, reason must be stated and by whom</i>
Comments:		

Date Closed:



Davenham Church of England Primary School

"Working Together, Playing Together, Serving God and Serving Others"

POLICY FOR DATA PROTECTION (GDPR)

Effective Date		16 October 2023	
Person Responsible		Joanne Hyslop	
Signed Headteacher	Signed Governors	Chair of	Date Ratified
J Hyslop	Martin Mewies		16 October 2023

