The Fenland Federation
Marshchapel Infant School
Grainthorpe Junior School

Data Protection Policy

Contents:

Statement of intent

The Fenland Federation is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially children's services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the school complies with the following core principles of the GDPR.

Organisational methods for keeping data secure are imperative, and **The Fenland Federation** believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy complies with the requirements set out in the GDPR, which will come into effect on 25 May 2018. The government have confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

If you have any enquiries in relation to this policy please contact the School Business Manager.

Further advice and information is available from the Information Commissioner's Office at www.ico.org.uk or 0303 123 1113.

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
- The School Standards and Framework Act 1998

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'

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

- Images & Videos Consent Document
- E-Safety Policy

2. Applicable data

2.1. For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

2.2. **Sensitive personal data** is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

3. Principles

3.1. There are 6 enforceable data protection principles contained in Article 5 of the General Data Protection regulations. They are key to compliance and The Fenland Federation will endeavour to ensure that they are adhered to at all times. The responsibility for adherence to the principles is the responsibility of **ALL** school staff.

3.1.1 Principle 1 – Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.

3.1.2 Principle 2 – Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3.1.3 Principle 3 – Personal data shall be adequate, relevant and limited to what is necessary.

3.1.4 Principle 4 – Personal data shall be accurate and where necessary kept up to date. Steps must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.

3.1.5 Principle 5 - Personal data shall be 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.

3.1.6 Principle 6 – Personal data shall be processed in a manner that ensures approprtiate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

3.2 To ensure compliance with the above principles The Fenland Federation will:

a) Produce an information asset register that contains details of the records it holds.
b) Inform individuals why the information is being collected at the point it is collected by way of privacy notices.
c) Inform individuals when their information is shared, and why and with whom it will be shared.
d) Check the quality and the accuracy of the information it holds.
e) Ensure that information is not retained for longer than is necessary.
f) Ensure that when obsolete information is destroyed and it is done so appropriately and securely.
g) Create, maintain and publish a Disposal and Retention Schedule setting out retention and disposal dates for common data sets and other information.
h) Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
i) Share information with others only when it is fair and lawful to do so and satisfies the lawful basis for processing that information.

j) Share personal data with other organisations for the purpose of crime prevention and/or detection, or for the purpose of legal proceedings, provided that the disclosure falls within an exemption to the non-disclosure provisions contained within the Data Protection Act 1998 or any subsequent legislation.
k) Disclose personal data where required to do so by law for example, following receipt of a court order.
l) Set out procedures to ensure compliance with the duty to respond to an individual's rights to:

- request access to personal information, known as Subject Access Requests.
- be informed about the way their data is used;
- have inaccurate personal data rectified;
- have their personal data erased;
- restrict the processing of their personal data; and
- object to the processing of their personal data.

m) Ensure our staff are appropriately and regularly trained and aware of and understand our policies and procedures.
n) Create and maintain a data breach notification spreadsheet to record data breaches and also circumstances where a breach was narrowly avoided.

4 Accountability

4.1 **The Fenland Federation** will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

4.2 The school will provide comprehensive, clear and transparent privacy notices.

4.3 Internal records of processing activities will include 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
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

4.4 The school will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation.
- Pseudonymisation.

- Transparency.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

4.5 Data protection impact assessments will be used, where appropriate.

5 Data protection officer (DPO)

5.1 A DPO will be appointed 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 An existing employee can be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

5.3 The individual appointed as DPO will have relevant training and knowledge of data protection law, particularly that in relation to schools.

5.4 The DPO will report to the highest level of management at the school, which is the Executive Headteacher.

5.5 The DPO will operate independently and will not be dismissed or penalised for performing their task.

5.6 Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

5.7 The DPO is Mr P Floyd, contact details available from the school office.

6 Lawful processing

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

6.2 The school will act as a data processor; however, this role may also be undertaken by other third parties.

6.3 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 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. (This condition is not available to processing undertaken by the school in the performance of its tasks.)

6.4 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.
- 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:
  - 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).

7 Consent

7.1 Consent will be sought prior to processing any data which cannot be done so under any other lawful basis, such as complying with a regulatory requirement.

7.2 Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

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

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

7.5 The school ensures 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.

7.6 Consent 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.

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

7.8 Where a child is under the age of 16 [or younger if the law provides it (up to the age of 13)], the consent of parents will be sought prior to the processing of their data, 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 School publishes a privacy notice on its website which provides information about how and why the school gathers and uses images and shares personal data.

8.2 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.

8.3 The privacy notice under the GDPR should include:

- Who you are and how they can contact you;
- The personal data you are collecting & why you are collecting it;
- Where you get the personal data from & who you are sharing it with;
- How long the data will be held for;
- Transfers to third countries and safeguards;
- Description of the data subjects individual rights;
- The data subjects right to withdraw consent for the processing of their data; and
- How individuals can complain.

8.4 The privacy notice will be reviewed at regular intervals to ensure it reflects current processing.

8.5 The privacy notice will be amended to reflect any changes to the way the School processes personal data.

8.6 Whilst the School will publish an overarching privacy notice it l will also issue a privacy notice to all parents and pupils, before, or as soon as possible after, any personal data relating to them is obtained. This may simply be an explanation why the information is being requested and the purpose for which it will be used.

8.7 The privacy notice will include details of how the School uses CCTV, whether it intends to use biometric data and how consent will be requested to do this and include details of the School's policy regarding photographs and electronic images of pupils.

8.8 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 contact details of the controller (the school), and where applicable, the controller's representative, as well as the DPO (not named).
- 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 a supervisory authority.
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

8.9 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.

8.10 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.

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

8.12 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.

9 The right of access

9.1 This section sets out the process that will be followed by the school when responding to requests for access to personal data made by the pupil or their parent or carer with Parental Responsibility.

9.2 There are two distinct rights of access to information held by schools about pupils, parents/carer and staff:

a) Pupils have a right to make a request under the GDPR to access the personal information held about them.
b) Pupils and parents or those with Parental Responsibility have a right to access the educational records. The right of those entitled to have access to curricular and educational records as defined within the Education (Pupil Information) (England) Regulations 2005.

9.3 Handling a subject access request for access to personal data:

9.3.1 Article 15 of the GDPR gives individuals the right to access personal data relating to them, processed by a data controller. The right can be exercised by a person with Parental Responsibility on behalf of their child dependent on the age and the understanding of the child. For the purposes of a subject access request the school will apply the full legal definition of 'Parental Responsibility' when determining who can access a child's personal data.

9.3.2 Requests for information must be made in writing; which can include e-mail, and be addressed to the Head Teacher or the Chair of Governors. If the original request does not clearly identify the information required, then the School will seek further enquiries to clarify what information is being requested.

9.3.3 The identity of the requestor must be established before the disclosure of any information is made. Proof of the relationship with the child (if not known) must also be established as this will verify whether the individual making the request can lawfully exercise that right on behalf of the child. Below are some examples of documents which can be used to establish identity:

- Passport
- Driving licence
- Utility bill with current address
- Birth/marriage certificate
- P45/P60
- Credit card or mortgage statement.

9.3.4 [It is widely accepted that children of primary school age do not have the maturity to understand and exercise their own rights and as such it is acceptable for those with Parental Responsibility to exercise these rights on their child's behalf. However, each request will be considered on its own merits and the circumstances surrounding the request and the child.] (Preceding section in brackets can be deleted or adapted to setting as appropriate) A child with competency to understand can refuse to consent to a request for their personal information made under the GDPR. This position differs when the request is for access to the Education Record of the child (see below for more detail).

9.3.5 No charge can be made for access to personal data that is not contained within an education record.

9.3.6 The response time for a subject access request is one month from the date of the request (irrespective of school holiday periods). The one month period will not commence until any necessary clarification of information is sought. The time to respond can be extended to two months where the request is complex or numerous.

9.3.7 There are some exemptions available under the Data Protection Act which will mean that occasionally personal data will need to be redacted (information blacked out/removed) or withheld from the disclosure. All information will be reviewed prior to disclosure to ensure that the intended disclosure complies with the School's legal obligations.

9.3.8 Where the personal data also relates to another individual who can be identified from the information, the information will be redacted to remove the information that identifies the third party. If it is not possible to separate the information relating to the third party from the information relating to the subject of the request, consideration will be given to withholding the information from disclosure. These considerations can be complex and additional advice will be sought when necessary.

9.3.9 Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another person will be withheld along with any information that would reveal that the child is at risk of abuse, or information relating to Court Proceedings.

9.3.10 Where redaction has taken place then a full copy of the information provided will be retained in order to maintain a record of what was redacted and why and a clear explanation of any redactions will be provided in the School's response to the request.

9.3.11 If there are concerns about the disclosure of information additional advice will be sought.

9.4 Handling a request for access to a curricular and educational record as defined within the Education (Pupil Information) (England) Regulations 2005.

9.4.1 A parent may make a request to access information contained within their child's education record, regardless of whether the child agrees to the disclosure of information to them. The right of access belongs to the parent in these cases. It is not a right being exercised by the parent on behalf of the child.

9.4.2 For the purpose of responding to an Educational Records request, the School will apply the definition of 'parent' contained within the Education Act 1996.

9.4.3 An "educational record" means any record of information which-

a. Is processed by or on behalf of the governing body of, or a teacher at, any school maintained by a local education authority and any special school which is not so maintained.
b. Relates to any person who is or has been a pupil at any such school; and
c. Originated from or was supplied by or on behalf of the persons specified in paragraph (a), other than information which is processed by a teacher solely for the teacher's own use

9.4.4 The amount that can be charged for a copy of information contained in an education record will depend upon the number of pages provided. The charge made will be in accordance with the Education (Pupil Information) (England) Regulations 2005.

9.4.5 No charge will be made to view the education record.

9.4.6 The response time for requests made under the Education (Pupil Information) (England) Regulations 2005 is 15 school days (this does not include half terms or teacher training days).

9.4.7 An exemption from the obligation to comply with the request will be claimed where the disclosure of the information to the parent may cause serious harm to the physical or mental or emotional condition of the pupil or another person or if the disclosure of the information would reveal that the child is at risk of abuse.

9.4.8 If a subject access request is made for information containing in whole or in part a pupils educational record a response must be provided within 15 school days

10 The right to rectification

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

10.2 Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.

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

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, the 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 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
- The personal data is processed in relation to the offer of information society services to a child

11.3 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

11.4 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.

11.5 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.

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, 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.

12.3 The 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 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

12.4 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.

12.5 The 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 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

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

13.5 The 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 The school is not required 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, the school will consider whether providing the information would prejudice the rights of any other individual.

13.9 The 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, 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 supervisory authority and to a judicial remedy.

14 The right to object

14.1 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.

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
- 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.
- 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.

14.4 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.

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, the 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, the school will offer a method for individuals to object online.

15 Privacy by design and privacy impact assessments

15.1 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.

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 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.

15.4 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.

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

15.6 High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- The use of CCTV.

15.7 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

15.8 Where a DPIA indicates high risk data processing, the school will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

16 Data Breaches

16.1 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.

16.2 The Executive Headteacher will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

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

16.4 All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it.

16.5 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.

16.6 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.

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

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

16.9 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.

16.10 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

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

17 Data security

17.1 The school will ensure only authorised individuals have access to personal data.

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

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

17.4 Digital data is password-protected on a network drive that is regularly backed up off-site.

17.5 All portable devices containing personal data will be encrypted.

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

17.7 Staff and governors will not save school files or data to personal computers or devices.

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

17.9 Staff must ensure that all personal devices used for accessing school files or email accounts are password-protected.

17.10 Storage of iPads and shared portable devices is secure and locked when not in daily use.

17.11 Emails containing sensitive or confidential information are encrypted between the sender and recipient if there are unsecure servers between the sender and the recipient.

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

17.13 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 the school premises accepts full responsibility for the security of the data. No personal data will be left unattended in any vehicles

17.14 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.

3.2. 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.

3.3. The physical security of the school's buildings and storage systems, and access to them, is reviewed on an annual basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

3.4. The Fenland Federation takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

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

3.6. The school will refer to any relevant guidance and seek advice where necessary if processing personal data utilising a cloud based solution.

18 CCTV and photography

18.1 Images and audio recordings of identifiable individuals captured by Closed Circuit Television amount to personal data relating to that individual and will be subject to the same provisions and safeguards afforded by the General Data Protection Regulations and the Data Protection Act as other types of recorded information.

18.2 The School will use CCTV for the following purposes:

- To protect the school buildings and assets;
- To increase personal safety of staff, pupils and visitors;
- To reduce the fear of crime;
- To support the Police in order to deter and detect and to apprehend and prosecute offenders;
- To help protect members of the public and private property;
- To investigate both pupil and staff behaviour where appropriate.

18.3 The School will ensure that any use of CCTV is necessary and proportionate to achieve the aims stated in 7.6 and will ensure that regular reviews of the use of CCTV within the School take place

18.4 The School will ensure that any use of CCTV is included in its records of data processing activity.

18.5 The School's use of CCTV will comply with the Information Commissioner's Office CCTV Code of Practice https://ico.org.uk/for-organisations/guide-to-data-protection/cctv/ .

18.6 The School will ensure that clear notices are in place identifying when an individual is entering an area that is monitored by CCTV. The notice will identify the School as the responsible data controller and will state the purpose for which the recording is taking place.

18.7 The School will not operate audio recording as part of the CCTV without seeking additional advice.

18.8 The School will not operate CCTV in any areas of the premises where individuals would have a legitimate expectation of personal privacy, such as toilets or changing rooms.

18.9 The School will ensure that CCTV recordings are kept securely and that access to them is restricted to those staff that operate the system or make decisions relating to how the images should be used.

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

18.11 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.

18.12 Precautions, as outlined in our **Images and Videos Consent Document**, are taken when publishing photographs of pupils, in print, video or on the school website.

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

19 Biometric Data

19.1 If the School uses or intends to use biometric data (such as fingerprint technology) a separate, detailed notice will be sent to all pupils and parents explaining the intended reasons for and lawful basis for the use of the data, and provide parents with options for alternative systems if they do not wish their child to provide this information and want to opt out.

19.2 The School will obtain the written consent of at least one parent or carer with Parental Responsibility for the child before taking and using any biometric data from a pupil.

20 Data retention

20.1 The governing body of the school will ensure that the school has an up to date and accurate retention and disposal schedule that is compliant with GDPR. The school will ensure that data is stored, transferred and disposed of securely an in accordance with the retention and disposal schedule.

20.2 Data will not be kept for longer than is necessary.

20.3 Unrequired data will be deleted as soon as practicable.

20.4 Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

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.

22 Complaints

22.1 Complaints relating to the school's compliance with GDPR will be dealt with in accordance with the school's complaints policy.

22.2 Complaints relating to personal information or access to education records should be made to the School Business Manager who will decide whether it is appropriate for the complaint to be dealt with through the school's complaints procedure. Complaints which are not appropriate to be dealt with through the school's complaints procedure can be referred to the Information Commissioner. Details of how to make a complaint to the ICO will be provided with the response letter. Reference to the ICO will only usually be made where the school's internal complaints process has been exhausted.

22.3 Complaints relating to information handling may be referred to the Information Commissioners Office (the statutory regulator). Contact details can be found on their website at www.ico.org.uk or 0303 123 1113.

23 Policy review

23.1 This policy is reviewed annually by the Executive Headteacher and the School Business Manager

23.2 This policy was adopted by The Fenland Federation at its Full Governing Body meeting in May 2018.

Compiled By: School Business Manager	**Revision number: 0**
Reviewed By: Executive Headteacher & Governors	**May 2018**
Approved By: Full Governing Body May 2018	
Review Date: May 2019	