Data Protection Policy

Status of policy: Statutory

Frequency of review: 2 years

Date of most recent review: Sept 2024

Date of next review: Sep 2026

Approved by FGB: 26th September 2026

1. Legal framework

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

- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA)
- School Standards and Framework Act 1998
- Freedom of Information Act 2000
- Electronic Commerce (EC Directive) Regulations 2002
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018)
- Protection of Freedoms Act 2012
- DfE (2024) 'Keeping children safe in education 2024'

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

- ICO (2022) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ICO (2012) 'IT asset disposal for organisations'
- DfE (2023) 'Data protection in schools'

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

- CCTV Policy
- Right of Access Policy
- Safeguarding 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 UK 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 UK GDPR as 'special categories of personal data', and is defined as:

- Genetic data.
- Biometric data.
- Data concerning health.
- Data concerning a person's sex life.
- Data concerning a person's sexual orientation.
- Personal data which reveals:
  - Racial or ethnic origin.
  - Political opinions.
  - Religious or philosophical beliefs.
  - Trade union membership.

- Principles.

2.3 ‘Sensitive personal data’ does not include data about criminal allegations, proceedings or convictions. In the case of criminal offence data, schools are only able to process this if it is either:

- Under the control of official authority; or
- Authorised by domestic law.

2.4 The latter point can only be used if the conditions of the reason for storing and requiring the data fall into one of the conditions below:

- The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller of the data subject in connection with employment, social security, social protection, health or social care purposes, public health, and research.

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

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2.6 The UK GDPR also requires that “the controller shall be responsible for, and able to demonstrate, compliance with” the above principles.

3. Accountability

3.1 The school will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR, and will provide comprehensive, clear and transparent privacy policies.

3.2 Records of activities relating to higher risk processing will be maintained, such as the processing of activities that:

- Are not occasional.
- Could result in a risk to the rights and freedoms of individuals.
- Involve the processing of special categories of data or criminal conviction and offence data.

3.3 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

3.4 The school will also document other aspects of compliance with the UK GDPR and DPA where this is deemed appropriate in certain circumstances by the DPO, including the following:

- Information required for privacy notices, e.g. the lawful basis for the processing
- Records of consent
- Controller-processor contracts
- The location of personal data
- Data Protection Impact Assessment (DPIA) reports
- Records of personal data breaches

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

- Minimising the processing of personal data.
- Pseudonymising personal data as soon as possible.
- Ensuring transparency in respect of the functions and processing of personal data.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

3.6 DPIAs will be used to identify and reduce data protection risks, where appropriate.

4. Data protection officer (DPO)

4.1 Parkgate Primary School has appointed a DPO in order to:

- Inform and advise Parkgate Primary School and its employees about their obligations to comply with the UK GDPR and other data protection laws.
- Monitor Parkgate Primary School's compliance with the UK 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.

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

4.3 Parkgate Primary School will make freely available the contact details for their appointed DPO:

Schools Data Protection Officer
Cheshire West and Chester Council,
4 Civic Way
Ellesmere Port
CH65 0BE

Email: schoolDPO@cheshirewestandchester.gov.uk

The DPO will operate independently, their role being to:

- advise the school and its employees about the obligations to comply with UK GDPR and other data protection requirements – 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 UK 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.

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

4.5 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.

5. Lawful processing

5.1 The legal basis for processing data will be identified and documented prior to data being processed. The school will make it clear, at all times, the basis on which personal data is processed.

5.2 Parkgate 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.

5.3 In addition, Parkgate Primary School will ensure that the processing of sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject.
- 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, t 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

6. Consent

6.1 Where there is no other legal basis for the processing of data Parkgate Primary School may rely on the consent of individuals, both parents and pupils, in seeking consent. Where used, consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

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

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

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

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

6.6 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.

7. The right to be informed

7.1 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.

7.2 If services are offered directly to a child, the school will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

7.3 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.

7.4 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.

8. The right of access

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

8.2 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 from the school office.

8.3 Parkgate 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.

8.4 A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.

8.5 Where a SAR has been made electronically, the information will be provided in a commonly used electronic format. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee may be charged.

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

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

8.8 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.

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

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

8.11 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.

8.12 The 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 *UK* GDPR during holiday periods, stating clearly how the school will handle these requests and how this may impact on any time scales.

9. The right to rectification

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

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

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

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

9.5 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.

10. The right to erasure

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

10.2 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

10.3 Parkgate 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

10.4 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.

10.5 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 where possible.

11. The right to restrict processing

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

11.2 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.

11.3 Parkgate 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 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

11.4 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.

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

12. The right to data portability

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

12.2 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.

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

- To personal data that an individual has provided to the 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

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

12.5 Parkgate Primary School is not obligated to adopt or maintain processing systems which are technically compatible with other organisations.

12.6 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.

12.7 Parkgate Primary School will respond to any requests for portability within one month.

12.8 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.

12.9 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.

13. The right to object

13.1 Parkgate 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.

13.2 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.

13.3 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.

13.4 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.

13.5 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.

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

14. Privacy by design and Data Protection Impact Assessments

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

14.2 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.

14.3 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.

14.4 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.

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

14.6 Parkgate 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

14.7 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 *UK* GDPR.

15. Data Processors

15.1 Parkgate Primary School will ensure that whenever it employs or utilises a data processor a written contract will be in place.

15.2 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 UK GDPR;
- assist the controller in meeting its UK 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 UK GDPR.

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

15.4 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.

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

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 Parkgate 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.

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 by the school's Data Protection Officer.

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 will be a breach of school policy and an additional breach of the UK GDPR.

17. Data security

17.1 Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access. Confidential paper records will not be left unattended or in clear view anywhere with general access.

17.2 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.

17.3 Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

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

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

17.6 All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

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

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

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

17.10 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.

17.11 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.

17.12 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.

17.13 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.

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

18. Safeguarding

18.1 The school understands that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe.

18.2 The school will ensure that staff have due regard to their ability to share personal information for safeguarding purposes, and that fears about sharing information must not be allowed to obstruct the need to safeguard and protect pupils. The governing board will ensure that staff are:

- Confident of the processing conditions which allow them to store and share information for safeguarding purposes, including information, which is sensitive and personal, and should be treated as 'special category personal data'.
- Aware that information can be shared without consent where there is good reason to do so, and the sharing of information will enhance the safeguarding of a pupil in a timely manner.

18.3 The school will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a child is shared with the relevant individuals or agencies proactively and as soon as is reasonably possible. Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the DSL will ensure that they record the following information:

- Whether data was shared
- What data was shared
- With whom data was shared
- For what reason data was shared

- Where a decision has been made not to seek consent from the data subject or their parent
- The reason that consent has not been sought, where appropriate

18.4 The school will aim to gain consent to share information where appropriate; however, staff will not endeavour to gain consent if to do so would place a child at risk. The school will manage all instances of data sharing for the purposes of keeping a child safe in line with the Child Protection and Safeguarding Policy.

18.5 Pupils' personal data will not be provided where the serious harm test is met. Where there is doubt, the school will seek independent legal advice.

19. Publication of information

19.1. Parkgate 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.

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

20. CCTV

20.1 Parkgate Primary School operates CCTV on the premises and is mindful of the UK GDPR implications of this. A separate CCTV policy is held by the school and is available for inspection on the school website.

20.2 Requests for access to CCTV are covered in both the CCTV policy, for general requests, and the Information Rights Policy, for Subject Access Requests.

21. Cloud computing

21.1 For the purposes of this policy, **'cloud computing'** refers to storing and accessing data and programs, such as documents, photos or videos, over the internet, rather than on a device's hard drive. Cloud computing involves the school accessing a shared pool of ICT services remotely via a private network or the internet.

21.2 All staff will be made aware of data protection requirements and how these are impacted by the storing of data in the cloud, including that cloud usage does not prevent data subjects from exercising their data protection rights.

22.2 If the cloud service offers an authentication process, each user will have their own account. A system will be implemented to allow user accounts to be created, updated, suspended and deleted, and for credentials to be reset if they are forgotten, lost or stolen. Access for employees will be removed when they leave the school.

22.3 All files and personal data will be encrypted before they leave a school device and are placed in the cloud, including when the data is 'in transit' between the device and

cloud. A robust encryption key management arrangement will be put in place to maintain protection of the encrypted data. The loss of an encryption key will be reported to the DPO immediately; failure to do so could result in accidental access or destruction of personal data and, therefore, a breach of the relevant data protection legislation.

22.4 As with files on school devices, only authorised parties will be able to access files on the cloud. An audit process will be put in place to alert the school should unauthorised access, deletion or modification occur, and ensure ongoing compliance with the school's policies for the use of cloud computing.

22.5 The school's usage of cloud computing, including the service's security and efficiency, will be assessed and monitored by the DPO. The DPO will also ensure that a contract and data processing agreement are in place with the service provider, confirming compliance with the principles of the UK GDPR and DPA. The agreement will specify the circumstances in which the service provider may access the personal data it processes, such as the provision of support services.

22.6 The DPO will also:

- Ensure that the service provider has completed a comprehensive and effective self-certification checklist covering data protection in the cloud.
- Ensure that the service provider can delete all copies of personal data within a timescale in line with the school's Data Protection Policy.
- Confirm that the service provider will remove all copies of data, including back-ups, if requested.
- Find out what will happen to personal data should the school decide to withdraw from the cloud service in the future.
- Assess the level of risk regarding network connectivity and make an informed decision as to whether the school is prepared to accept that risk.
- Monitor the use of the school's cloud service, with any suspicious or inappropriate behaviour of pupils, staff or parents being reported directly to the headteacher

21. Data retention

21.1 Data will not be kept for longer than is necessary in line with the schools Record Management Policy. Unrequired data will be deleted as soon as practicable.

21.2 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.

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

22. DBS data

22.1 All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication. Data provided by the DBS will never be duplicated.

22.2 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.