Data Protection Policy

New End Primary School

Date Reviewed: **Autumn Term 2023**
Review Date: **Autumn Term 2025**
(unless advised to review earlier by Camden)

Adapted from Camden's Policy

Contents:

1. Aims

a. New End Primary School aims to ensure that all personal data collected, stored, processed and destroyed about any natural person, whether they be a member of staff, pupil, parent, Governor, visitors, contractor, consultant, or any other individual is done so in accordance with the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA 2018).

b. This policy applies to all personal data, regardless of whether it is in paper or electronic format, or the type of filing system it is stored in, and whether the collection or processing of data was, or is, in any way automated.

2. Legislation and guidance

a. This policy meets the current requirements of UK Data Protection legislation. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR, UK GDPR and DPA 2018. It is also based on the information provided by the Article 29 Working Party.

b. Additionally, it meets the requirements of the Protection of Freedoms Act 2012, ICO's code of practice in relation to CCTV usage, and the DBS Code of Practice in relation to handling sensitive information. This policy complies with the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Data controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data processor	A natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller, following the Controller's instruction.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Consent	Freely given, specific, informed and unambiguous indication of the data subject's wishes via a statement or by a clear affirmative action, signifying agreement to a specific processing of personal data relating to them.

Personal data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to 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.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including Information about an individual's: ● Racial or ethnic origin ● Political opinions ● Religious or philosophical beliefs ● Trade union membership ● Genetics ● Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes ● Health – physical or mental ● Sex life or sexual orientation ● History of offences, convictions or cautions * * Note: Whilst criminal offences are not listed as special category data, within this policy they are regarded as such in acknowledgment of the extra care that is needed with this data set.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing can be automated or manual.
Data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

a. The School collects and determines the processing for personal data relating to parents/carers, pupils, the school workforce, governors, visitors and others, in addition they process data on the behalf of others therefore is a data controller and a data processor.

b. The School is registered as a data controller with the ICO and will renew this registration as legally required, the registration number is **Z7081754**.

5. Roles and responsibilities

a. This policy applies to all individuals employed by our school, and to external organisations or individuals working on our behalf. Employees who do not comply with this policy may face disciplinary action.

b. **Governing Board:** The Governing Board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

c. **Data Protection Officer:** The School has appointed Andrew Maughan, Borough Solicitor for the London Borough of Camden as Data Protection Officer (DPO). He can be contacted at schooldpo@camden.gov.uk or 0207 974 4365. The DPO is supported by Data Protection Advisors that monitor these contact details and carry out business-as-usual tasks on his behalf.

They are responsible for overseeing the implementation of this policy, along with any future development of this or related policies/guidelines, and reviewing our compliance with data protection law.

The DPO Team provide support to the school in relation to compliance status and make recommendations on data protection issues.

The DPO is a named point of contact for all Data Subjects whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their SLA for Service

d. **Representative of the data controller:** The head teacher (Karyn Ray) – contact head@newend.camden.sch.uk – acts as the representative of the data controller on a day-to-day basis.

e. **All Staff:** staff (regardless of role) are responsible for:

i. Collecting, storing and processing any personal data in accordance with this policy
ii. Informing the school of any changes to their personal data, e.g. a change of address, telephone number, or bank details.
iii. Reporting a Data Breach, Data Right Request, or Freedom of Information Request.
iv. Contacting the Data Protection Lead in school (Head teacher):
    1. With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    2. If they have any concerns that this policy is not being followed
    3. If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    4. If they need to rely on or capture consent, draft a privacy notice/notification, or transfer personal data outside the United Kingdom.
    5. Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    6. If they need help with any contracts or sharing personal data with third parties

6. The Data protection principles

a. Data Protection is based on seven principles that the School must comply with. These are that data must be;
   i. Processed lawfully, fairly and in a transparent manner.
   ii. Collected for specified, explicit and legitimate purposes.
   iii. Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
   iv. Accurate and, where necessary, kept up-to-date.
   v. Kept for no longer than is necessary for the purposes for which it is processed.
   vi. Processed in a way that ensures it is appropriately secure.
   vii. The Accountability principle ties these all together by requiring an organisation to take responsibility for complying with the other six principles. Including having appropriate measures and records in place to be able to demonstrate compliance. This policy sets out how New End Primary aims to comply with these key principles.

7. Processing personal data

a. **Fair, lawful and transparent:**

   i. The school will only process personal data in ways that would reasonably be expected of a school and will be honest and transparent about the reasons for any processing. We will only process personal data where we have one of six lawful bases (legal reasons) to do so under data protection law:

      1. The individual (or their parent/carer when appropriate) has freely given clear **consent**
      2. The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
      3. The data needs to be processed so that the school can **comply with a legal obligation**
      4. The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
      5. The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest**, and carry out its official functions
      6. The data needs to be processed for the **legitimate interests of the school** or a third party (provided the individual's rights and freedoms are not overridden)

   ii. For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in data protection law. These are where:

      1. The individual (or their parent / carer in the case of a pupil, where appropriate) has **given explicit consent**;
      2. It is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment of a Data Controller or of a Data Subject;
      3. It is necessary to protect the **vital interests** of the Data Subject;
      4. Processing is carried out in the course of its **legitimate activities** with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim;
      5. The Personal Data has **manifestly been made public** by the Data Subject;
      6. There is the **establishment, exercise or defence of a legal claim**;
      7. There are reasons of **public interest** in the area of **public health**;
      8. Processing is necessary for the purposes of preventative or occupational medicine (e.g. for the **assessment of the working capacity of the employee**, the medical diagnosis, the provision of health or social care or treatment);

9. There are **archiving** purposes **in the public interest**.

iii. Where we collect personal data directly from individuals, we will provide them with the relevant information required by data protection law, in the form of a Privacy Notice. The privacy notices for pupils and parents/Carers, and for visitors to the school can be found on the school website. Hard copies can be requested from the school office. A hard copy of the School Workforce Privacy Notice will be added to the staff handbook.

b. **Limitation, minimisation and accuracy:**

i. The school will not collect more data than it requires. For significant processing activities, the Information Asset Owners listed in the Information Asset Register will be responsible for ensuring that only the minimum information required for the specific purpose is held, and no more.
ii. We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data in our privacy notices.
iii. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.
iv. Staff must only access and process personal data where it is necessary to do their jobs.
v. We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.
vi. When personal data is longer required, staff must ensure it is destroyed. This will be done in accordance with the school document retention & destruction policy, which states how long particular documents should be kept, and how they should be destroyed.
vii. Copies of the retention & destruction policy can be found on the school website (www.newend.camden.sch.uk).

8. Sharing personal data

a. In order to efficiently, effectively and legally function as a data controller we are required to share information with appropriate third parties, including but not limited to situations where:

i. There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
ii. We need to liaise with other agencies or services – we may seek consent when appropriate before doing this where possible.
iii. Our suppliers or contractors need data to enable us to provide services to our employees and pupils – for example, IT companies. When doing this, we will:
    1. Only appoint suppliers or contractors who can provide sufficient guarantees that they comply with data protection law and have satisfactory security measures in place.
    2. Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
    3. Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

b. We will also share personal data with law enforcement and government bodies when required to do so, these include, but are not limited to:

i. The prevention or detection of crime and/or fraud
ii. The apprehension or prosecution of offenders
iii. The assessment or collection of tax owed to HMRC
iv. In connection with legal proceedings
v. Where the disclosure is required to satisfy our safeguarding obligations
vi. Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

c. We may also share personal data with emergency services and local authorities to help them to respond to an emergency that affects any of our pupils or staff.

9. Transferring Data Internationally

a. We may send your information to other countries where:

   i. We, or a company we work with, store information on computer servers based overseas; or
   ii. We communicate with you when you are overseas.

b. We conduct due diligence on the companies we share data with and note whether they process data in the UK, EEA (which means the European Union, Liechtenstein, Norway and Iceland) or outside of the EEA.
c. The UK and countries in the EEA are obliged to adhere to the requirements of the GDPR and have equivalent legislation that confers the same level of protection to your personal data.
d. For organisations who process data outside the UK and EEA we will assess the circumstances and ensure there is no undue risk.
e. Additionally, we will assess if there are adequate legal provisions in place to transfer data outside of the UK.

10. Individuals' Data Protection Rights

a. **Access Rights:** individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them. If a subject access request is received, and if we hold information on that individual, we will:

   i. Give a description of it.
   ii. Tell them why we are holding and processing it, and how long we will keep it for.
   iii. Explain where we got it from, if not from them.
   iv. Tell them who it has been, or will be, shared with.
   v. Let them know whether any automated decision-making is being applied to the data, and any consequences of this.
   vi. NOT provide information where it compromises the privacy of others.
   vii. Or, give a copy of the information in an intelligible form.

b. **Other Rights regarding your Data** include an individual's right to:

   i. Withdraw their consent to processing at any time, this only relates to tasks where the school relies on consent to process the data.
   ii. Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it in certain circumstances and where sufficient supporting evidence is supplied.
   iii. Prevent the use of their personal data for direct marketing.
   iv. Challenge processing which has been justified based on public interest, official authority or legitimate interests.
   v. Request a copy of agreements under which their personal data is transferred outside of the European Economic Area.
   vi. Object to decisions based solely on automated decision-making or profiling (decisions taken with no human involvement, which might negatively affect them).
   vii. Request a cease to any processing that is likely to cause damage or distress.
   viii. Be notified of a data breach in certain circumstances.
   ix. Refer a complaint to the ICO.
   x. Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

In most cases, we will respond to requests within 1 month, as required under data protection legislation. However, we are able to extend this period by up to 2 months for complex requests or exceptional circumstances.

We reserve the right to verify the requester's identification by asking for Photo ID, if this proves insufficient then further ID may be required.

To exercise any of the rights or requests listed above, requester should contact the school office by emailing admin@newend.camden.sch.uk or by phoning 0207 431 0961.

While New End Primary will comply with the Data Protection legislation when dealing with all data requests submitted in any format, individuals are asked to submit their request in written format to assist with comprehension. They should include:

1. Name of individual
2. Correspondence address
3. Contact number and email address
4. Details of the request

If staff receive a subject access request, they must immediately forward it to the School Business Manager.

c. **Children and Data Rights/Requests**

i. An individual's data belongs to them therefore a child's data belongs to that child, and not the child's parents or carers.
ii. However, children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of invoking a data request. Therefore, for children under the age of 12, most data requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.
iii. Where a child is judged to be of sufficient age and maturity to exercise their rights and a request is invoked on their behalf, we would require them to give consent to authorise the action to be undertaken.

d. **Responding to subject access requests**

i. When responding to requests, we will not disclose information if it:
    1. Might cause serious harm to the physical or mental health of the pupil or another individual; or
    2. Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests; or
    3. Is contained in adoption or parental order records; or
    4. Is given to a court in proceedings concerning the child
ii. If the request is manifestly unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which would only take into account administrative costs..
iii. A request will be deemed manifestly unfounded or excessive if it is repetitive or asks for further copies of the same information.
iv. In the event we refuse a request, we will tell the individual why, and tell them they have the right to refer a complaint to the ICO.

11. Parental requests to see the educational record

a. Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

b. Requests should be made in writing to the School Business Manager- bursar@newend.camden.sch.com, and should include:
    i. Name of individual
    ii. Correspondence address
    iii. Contact number and email address

12. Close Circuit Television (CCTV)

a. The school uses CCTV for the purposes of:
    i. Monitoring the main pedestrian entrance to the school and allowing office staff to observe visitors
    ii. Security and crime prevention
    iii. There is one CCTV camera viewing the main pedestrian entrance. The CCTV image is not recorded.
    iv. The school's CCTV manager is the SBM who is responsible for ensuing day-to-day that CCTV is managed in line with the ICOs CCTV code of conduct.

13. Photographs and videos

a. As part of our school activities, we may take photographs and record images of individuals within our school.
b. The use of school photographs includes but is not limited to:
    i. Within school on notice boards and in school brochures, newsletters and prospectuses.
    ii. Outside of school by external agencies and partners such as the school photographer, local and national newspapers and local and national campaigns we are involved with
    iii. Online on our website or social media pages
c. New End Primary will obtain consent from the responsible individuals to use pupil images. When doing so we will clearly explain how the photograph and/or video will be collected and used to both the parent/carer and pupil when obtaining consent.
d. Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.
e. Consent can be withdrawn, in writing, by contacting the school office (admin@newend.camden.sch.uk).
f. When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified. Please refer to our Safeguarding & Child Protection Policy on the school website for more information on our use of photographs and videos.

14. Data protection by design and default

a. We will put measures in place to show that we have integrated data protection into all of our data collection and processing activities. These include, but are not limited to the following organisational and technical measures:
    i. Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
    ii. Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection regulations.
    iii. Completing data privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies or processing tools. Advice and guidance will be sought from the DPO.
    iv. Integrating data protection into internal documents including this policy, any related policies and privacy notices
    v. Regular training for the school workforce on data protection law, this policy and any related policies and any other data protection matters. Records of attendance will be kept to ensure that all data handlers receive appropriate training.
    vi. Periodic audits will be undertaken to monitor and review our privacy measures and make sure we are compliant.

vii. Maintaining records of our processing activities, including:
    1. For the benefit of data subjects, making available the name and contact details of our school DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    2. For all personal data that we hold; maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

15. Information Asset Register

a. The school is required by Article 30 of the GDPR to keep a record of data processing activities. This is maintained in an Information Asset Register.
b. For each Asset listed in the register, there will be specified:
    i. The purposes the information is used for.
    ii. The categories of data subjects (e.g. students, parents, staff)
    iii. The categories of personal data (e.g. contact details, educational records, employment records)
    iv. The retention period for that data, or link to the retention and destruction policy.
    v. Details of any transfers to international organisations or third party countries.
    vi. Security measures protecting the data
    vii. The condition(s) under Article 6 and/or Article 9 of the GDPR that allow the processing
    viii. The lawful basis relied on for the processing
    ix. The details of any joint Data Controllers
    x. The information necessary to demonstrate compliance with any of the other functions referred to in this policy. e.g. Sections 4 through 9.
    xi. The Information Asset Owner (IAO)
c. The maintenance of this register will be overseen by the School Business Manager and the responsibility for ensuring each entry remains accurate and is regularly reviewed lies with the corresponding IAO.

16. Data security and storage of records

a. We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.
b. Our organisational and technical measures include, but are not limited to;
    i. Paper-based records and portable electronic devices, such as laptops, tablets and hard drives that contain personal data being kept under lock and key when not in use. We encourage, where possible, a clear desk policy.
    ii. See Appendix 2. *10 Golden Rules for Information Security in Schools*.
    iii. Papers containing confidential personal data will not be left out on display when not in use unless there is a compelling lawful basis to do so e.g. Public Task to display Allergy information.
    iv. Passwords that are at least eight characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals.
    v. Encryption software is used to protect any devices such as Laptops, Tablets and USB Devices where saving to the hard drive is enabled.
    vi. Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see LGfL Online safety policy, and staff code of conduct*)*
    vii. Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

17. Disposal of records

a. Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will be rectified or updated, unless it is no longer of use and therefore will be disposed of securely.
b. For example, we will shred paper-based records, and overwrite or delete electronic files. We may also use a third party to dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law and provide a certificate of destruction.
c. When records are disposed of, as part of the Data Retention schedule, this is then recorded on our record of destruction log.

18. Personal data breaches

a. The school will make all reasonable endeavours to ensure that there are no personal data breaches.
b. All potential or confirmed Data Breach incidents should be reported to the School Business Manager or Head teacher where they will be assigned a unique reference number and recorded in the school's data breach log.
c. Once logged, incidents will then be investigated, the potential impact assessed, and appropriate remedial action undertaken. The DPO will be consulted as required.
d. In the event of a data breach, we will follow the procedure set out in the school's Breach Management Policy (see Appendix 1.). Where appropriate, we will report the data breach to the ICO and affected Data Subjects within 72 hours.
e. Examples of a Data Protection Breach include but are not limited to:
    i. Personal data being left unattended in an office, a classroom or the staffroom
    ii. Sending information relating to a pupil or family to the wrong member of staff in school, or to the wrong parent
    iii. A non-anonymised dataset being published on the school website eg. showing the exam results of pupils eligible for the pupil premium
    iv. Safeguarding information being made available to an unauthorised person
    v. The theft of a school laptop containing non-encrypted personal data about pupils

19. Monitoring arrangements

a. The DPO is responsible for monitoring and reviewing this policy as part of the general auditing and compliance work, they carry out.
b. They will work with School Data Protection Lead (the headteacher) to ensure that this policy remains contemporaneous and appropriate.
c. This policy will be reviewed annually by staff in school, and changes recommended when appropriate. The Governors will be asked to sign off the policy review and any necessary changes.

20. Links with other policies

a. This data protection policy is linked to our:
    i. Freedom of Information publication scheme
    ii. Online Safety Policy
    iii. Data Retention Schedule
    iv. Breach reporting protocol (Appendix 1.)
    v. Disaster Recovery/Business Continuity Plan
    vi. Safeguarding and Child Protection Policy

Appendix 1: New End Primary School – Data Breach Management Policy

1. This procedure is based on guidance on personal data breaches produced by the ICO and the Article 29 Working Party.

2. On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO. Within the school, this will be done through the head teacher.

3. The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    a. Lost
    b. Stolen
    c. Destroyed
    d. Altered
    e. Disclosed or made available where it should not have been
    f. Made available to unauthorised people

4. After investigating, the DPO will alert the head teacher and chair of governors where deemed appropriate.

5. The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.

6. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.

7. The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    a. Loss of control over their data
    b. Discrimination
    c. Identify theft or fraud
    d. Financial loss
    e. Unauthorised reversal of pseudonymisation (for example, key-coding)
    f. Damage to reputation
    g. Loss of confidentiality
    h. Any other significant economic or social disadvantage to the individual(s) concerned

    If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

8. The DPO will document the decision (either way); in case it is challenged later by the ICO or an individual affected by the breach. Documented decisions are stored on the internal school breach register, and in the school electronic and paper filing systems. Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    a. A description of the nature of the personal data breach including, where possible:
        i. The categories and approximate number of individuals concerned
        ii. The categories and approximate number of personal data records concerned o The name and contact details of the DPO
    b. A description of the likely consequences of the personal data breach
    c. A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

9. If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

10. The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    a. The name and contact details of the DPO
    b. A description of the likely consequences of the personal data breach
    c. A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

11. The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

12. The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    a. Facts and cause
    b. Effects
    c. Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
    d. Records of all breaches will be stored on the internal school breach register, and in the school electronic and paper filing systems.

13. The DPO and head teacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

14. **Actions to minimise the impact of data breaches:** The school will take actions to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. The school will review the effectiveness of these actions and amend them as necessary after any data breach. Such actions include, but are not limited to;
    a. Anonymising and minimising data
    b. Encrypted drives
    c. Secure access servers
    d. Strong password setting
    e. Training and support for staff and governors
    f. Encrypted email.

Appendix 2. Ten Golden Rules for Information Security in Schools

1. Never disclose or share your User id, passwords or any other credentials with anyone else.
2. Do not open email attachments from unknown or suspicious sources.
3. Ensure that all information held on portable devices including laptops, memory sticks and other devices are stored in accordance with the School's data handling policies.
4. Remember never leave your computer signed on while unattended. You are responsible for all actions carried out under your Log-on, so Log-off when leaving your computer out of sight.
5. Maintain a secure workspace, do not leave confidential or sensitive information on your desk or on printers or photocopiers and lock it away securely. Keep classroom doors closed when not in the room. Ensure that confidential waste is disposed of in accordance with School procedures.
6. Do not install software and devices onto the School's network and systems. Your IT provider should install authorised software.
7. Save all information to network drives to ensure that this information is backed-up. Where appropriate, store sensitive and confidential information on secured drives/encrypted USB sticks.
8. Do not share or disclose information with third parties unless certain that it is appropriate to do so. Make sure this is sent securely.
9. Make sure that when you take information offsite it is appropriately secured. Be extra vigilant when transporting this information in public places. Only take information offsite if you have to and refer to the School policy.
10. Ensure that equipment, records and other devices are returned when you cease employment with the school.