THE MINSTER
NURSERY AND INFANT SCHOOL
SCHOOL OF INSPIRATION
DETERMINATION HONOUR BELIEVE
PREPARING FOR A BRIGHT FUTURE WITH INNOVATIVE AND EXCITING LEARNING

Data Protection, Privacy and Information Systems Policy 2018

Approved at FGB Meeting 00/00/19	Chair of Governing Body	Signed ……../……../…….
Approved at Resources Committee	Chair of Resources	Signed ……../……../…….

To be reviewed on or before October 2019

Please see end of document for version control

Version 27/03/2018 09:22

Table of Contents

Head Teacher's Introduction 5
Policy Framework 6
Lawful Basis 6
Purpose 6
Scope 7
GDPR 7
The 6 Data Protection Principles 8
Types of Data 9
Information and Data Sharing 10
Risk 11
Choice and Consent 11
Subject Access Requests 12
Data Management 13
General Processing Procedure 15
Implementation 15
Remote and Mobile Working 16
Good Office Practice 18
IT Infrastructure Security 19
Training and Awareness 20
Notification to the Information Commissioner's Office 20
Financial Penalties, Criminal Offence & Data Breaches 20
Policy Compliance 21
Policy Governance 21
Review and Revision 22
Appendix 22

Head Teacher's Introduction

Introduction

The pan–European General Data Protection Regulation became enforceable as part of The Data Protection Act in May 2018. It is designed to ensure individuals, their identities and their privacy are protected against the many ways data can be collected and used. We have new responsibilities as individuals, employers, employees and as an organisation, to ensure data is secure and only used for agreed and limited purposes and that the rights and privacy of the individual remain paramount in the design and implementation of all data handling.

We see GDPR as an opportunity to improve general processes and methods of achieving good administrative and curricula results, in tandem with our schoolwide initiatives to encourage all staff members to take full ownership for change, improvement and higher standards.

There is a continuing element of culture change as we move toward a 'privacy by design' model of working and incorporate the accountability principle (see Page 7) and the idea of inbuilt demonstrability of compliance in everything we do with data.

Our school Data Protection Policy will remain a live document while excellent models of practice are agreed nationally for mainstream schools. Therefore review dates will be set more often regularly than usual until new processes have settled in.

The latest updates have incorporated recommendations and suggestions from our visit from an advisory team from the Information Commissioner's Office (ICO) in July 2018 and additional suggestions arising from our DPO Service Audit in October 2018.

Mrs Stephanie Edmonds
Head Teacher
The Minster Nursery & Infant School

Policy Framework

The Minster Nursery & Infant School holds a great deal of personal information and must ensure that this information is kept safe and is managed securely. The school has a duty under the General Data Protection Regulation, which has been incorporated into the new Data Protection Act 2018, to ensure that appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. The General Data Protection Regulation (referred to as the GDPR in this document) strengthens and extends individual rights and organizational responsibilities to protect the privacy of individuals.

The GDPR provides an opportunity to consolidate our policies and make the overall framework more coherent. The Record Keeping and Retention Policy and cybersecurity procedure are now incorporated under the greater *privacy umbrella* of this policy.

Data comprises those documents which facilitate the business carried out by the school and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. Data includes hand written notes, notices, paper printed or electronic documents.

Lawful Basis

We are required to specify the lawful basis on which the school relies for processing different data

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/public-task/

The legal basis for the bulk of the school's processing is 'in the exercise of official authority' as a public task, set out in law as in the public interest.
Therefore the school does not need a specific statutory power to process personal data, but we are obliged to have a clear basis in law for each discrete type of processing we pursue.
All processing must be necessary. We are obliged to remain vigilant of the fact that we lose that lawful basis to processing data if we could reasonably be expected to be able to perform our tasks or exercise our powers in a less intrusive way for any particular activity.
We document here, our decision to rely on this statutory basis as demonstration of compliance and refer to it in relation to any particular task, function or power as may be required by the Information Commissioner's Office (ICO).

Purpose

The school is committed to privacy by design in our approach to all personal information (https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/) as advocated by the GDPR and the Information Commissioner's Office.

This approach to administrative tasks promotes privacy and data protection compliance as integral to the school's ethos and not to be seen as a *bolt-on* or *after-thought*. Alterations and improvements to our policies and procedures will embody this dictum.

There are strict obligations over data that the school can hold, and now under the GDPR, there has to be verifiable evidence of knowing what we are keeping, how we are keeping it, why we are keeping it and how we intend to dispose of data on any identifiable individual. The new law has many permutations but now specifically includes any written information to be classed as data, what can be seen by any person such as on an office wall or left in any readable form where an unauthorised person might read it constitutes a data breach for which there must be purposeful and documented responses and plans for damage limitation to individuals and the organisation.

Therefore, new legislation provides us with a new opportunity, as well as an obligation to apply, a more rigorous approach to privacy rights, transparency and accountability.

Pre-eminently, the GDPR gives far more rights to the individual and his or her choices in what happens to their data and its usage.

Scope

This document sets out obligations for all school staff members as well as agency workers, contractual third parties and agents of the school who have access to personal data/information processed by the schools. This includes the storage, transportation, use and disposal of information and redundant IT equipment outside of the schools environment, the physical security of servers and server access where data is held. It may also overlap with other policies including Confidentiality and Acceptable Use Policies, which remain separate but work in conjunction with this policy. Under the GDPR it also includes any sharing of data with 3rd parties and whether we are tracking and recording all changes additions to such arrangements and properly assessing these via a Privacy Impact Assessment (PIA) which can be produced in chronology of other PIAs for external statutory inspection.

GDPR

The General Data Protection Regulation has replaced and superseded The Data Protection Act 1998. This is to be embodied in a new Data Protection Bill before Parliament in 2018. The Freedom of Information (FOI) Act will still hold even though many aspects of one mirror the other. GDPR is now the primary legislation in the United Kingdom which regulates the processing of information /data about living individuals – these are referred to as Data Subjects.

Processing includes the obtaining, holding, use or disclosure of that information. The Minster Nursery & Infant School, as ***Data Controller*** has a duty to process personal data in compliance with the provisions of the Regulation. All those who provide services on behalf of the School and their *Processors* (organisations that process data on behalf of the Schools) must also comply with the Act and this must verified by the school with issuing of a fresh contract if necessary to specify this.

Under GDPR, Subject Access Requests (SARs) are given more legal standing on behalf of individuals. This means that anyone who has information stored about them can request to know what that data is (see Page 8). Only vexatious demands can be denied but the reasons for such a refusal would have to be made clearly, recorded and be subject to scrutiny by the Information Commissioner's Office (see Page 6).

The 7 Data Protection Principles

The 8 Principles of the DPA have been replaced by 6 Key Principles under GDPR

Data must be:

a) **processed lawfully, fairly and in a transparent manner** in relation to individuals;

- The school must ensure that all parties are aware of their rights and understand how their data is being used, kept securely and will be disposed of when no longer required.

b) **collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes**; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

- The school will ensure that collected and received data is only used for the purposes set out for its prime remit unless fully explained to all affected data subjects

c) **adequate, relevant and limited** to what is necessary in relation to the purposes for which they are processed;

- The School or its processors cannot use data set up fresh activities not covered by the initial legal basis or consent.

d) **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;

- The School or its processors must recognise that any inaccuracy is a data breach. Relatively fluid data such as contact phone numbers must be up to date and left blank if there is any uncertainty (illegible writing etc.)

e) **kept in a form which permits identification of data subjects for no longer than is necessary** for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

- The school has processes in place to anonymise data as soon as it is solely required for statistical purposes. Photography and Film will be deleted at the earliest opportunity and the Retention procedure adhered to. (Appendix E)

f) **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.

g) **Accountability Principle – Demonstrating Compliance**

We are additionally required as an organisation to demonstrate how we comply with principles above. Please see ***Policy Compliance*** and ***Policy Governance*** (Page 19).

see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/

Types of Data

Data as defined under the Act may include both facts and opinions about individuals. It also includes information regarding the intentions of the Data Controller (i.e. the School) towards the individual.

There are two types of data defined:

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;
Includes IP addresses and mobile device IDs

Sensitive Data - data relating to race or ethnic origin, political opinions, religious or other beliefs, trade union membership; health; sex life, criminal proceedings or convictions of an individual. Sensitive Personal Data now comes under Special Categories of personal data within the terms of GDPR and merits higher protection.

Child Protection

Child Protection (The Children's Act 2004) supersedes any other directive and does not require the consent of any party.

Religious Preference

Religious Preference is recorded at entry for prioritization of Churches Together, That data is used additionally to notify teachers of special consideration where class activity may have a bearing on their religion or vice versa. Additionally, a parent or carer may request the school excuse a child from certain events or celebrations.

Information and Data Sharing

The legal basis for sharing information with other statutory organisations or 3rd party suppliers is Public Interest

The school will ensure appropriate use of data sharing by following the seven golden rules for information-sharing

1. Remember that the Data Protection Act is not a barrier to sharing information **but provides a framework to ensure that personal information about living persons is shared appropriately.**

2. Be open and honest **with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be, shared, and seek their agreement, unless it is unsafe or inappropriate to do so.**

3. Seek advice **if you are in any doubt, without disclosing the identity of the person where possible.**

4. Share with consent where appropriate **and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.**

5. Consider safety and wellbeing: **base your information-sharing decisions on considerations of the safety and wellbeing of the person and others who may be affected by their actions.**

6. Necessary, proportionate, relevant, accurate, timely and secure: **ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up to date, is shared in a timely fashion, and is shared securely.**

7. Keep a record **of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.**

Risk

We aim to minimize the likelihood of, and mitigate the effects of, data breaches when they occur as they may result in:

- Unauthorised access to personal and sensitive information.
- Potential sanctions against the Schools or individuals imposed by the Information Commissioner's Office as a result of a poor response to, or poor preparation for, information loss or misuse (known as a breach).
- Potential legal action against the Schools or individuals as a result of information loss or misuse.
- Schools reputational damage as a result of information loss or misuse.
- Destruction & Loss of Data

The school has established a **Data Risk Schedule (see Appendix H)** which is part of the **General Risk Register** in which to identify the array of risk associated with the different types of data collection and processing within the school.

Data Flow Audits and gap analyses of discrete activities with risk potential will be carried out. A Privacy Impact Assessment will be used to highlight areas of weakness and to suggest strategies for mitigating, and responding to, data breaches. This is a much more stringent area of GDPR which we will be incorporating into all areas of school activity. In order to help us with this task we are using GDPRis software that allows us to maintain all the monitoring and self-appraisal data in one centrally identified location.

Choice and Consent

The school's legal basis for processing data is largely covered by 'Public Interest' as laid down by the GDPR (see Page One: Lawful Basis). Consent can and should be seen as an opportunity to give Parents and Carers reassurance about the privacy of their data and a sense of control and trust in the process of gaining additional support for what uses are being made of photos, films and additional data. This in turn should enhance our reputation for professionalism and being consultative in a partnership relationship with parents and carers.

Two types of data collected in the school require that Parental/Carer consent be sought to carry out additional gathering and handling or are recognized as potentially invasive or that may jeopardise personal privacy:

1. **Photography and Film Consent:** We also ensure full consent is agreed for each type of use made of a child's image or video in which they appear. We will inform parents and carers how information about them is being used and how it may be shared and with whom (see Appendix C – Photography & Film Consent Form). A clear explanation as to how consent can be withdrawn is set out on the consent form to ensure a wholly voluntary arrangement has been made. There is a link on the school website to the Consent Withdrawal Form (Appendix D) so that granular alteration can be made as well as a complete change of consent.
2. **Tapestry Consent:** Nursery & Reception use Tapestry – an online child development assessment tool for which we ask parents to sign an additional consent form (see Appendix L)

Subject Access Requests

A formal request for access to records under the Act is known as a ***Subject Access Request*** or ***SAR***. The individuals to whom the data relates (data subject) may make a subject access request either personally or through legally approved representatives such as a solicitor or advice worker (although they will be asked for evidence that they are acting on behalf of the data subject). The school will also request relevant proof of identity.

In cases where data subjects are incapable of understanding or exercising their rights, e.g. they are too young or are suffering from a disability which limits their understanding, then subject access requests may be made by parents or other persons who are legally able to act on behalf of the data subject in law. This is the usual lawful way in which will operate as a school for young children.

Where a data subject makes a SAR, the schools have a legal responsibility to provide a copy of these records. This can be a complex process determining what records are legally accessible, what exemptions may apply and then making the information available.

A SAR (Subject Access Request) can be made verbally or in writing (including via email) to include:

- Name and address
- Description of what is being requested

The requestor is required to supply such information as may be *reasonably* required in order to identify them and to enable the information to be located. This can be transferred to paper by a member of staff or completed by the requestor, her or himself.

The school is required to respond without delay within 1 month with either:

- requested information in permanent form; or
- requested information in some other form agreed by applicant; or
- refusal to disclose (give reasons for decision and inform applicant of right to complain to Information Commissioner); or confirmation or denial of processing of information
- The school has the right to refuse a ‘vexatious’ request but must be able to justify such a decision
- A charge may be levied for a request if it is deemed to be repetitious or excessive.

The one month period commences when the school has received proof of identity which ensures data security.

Data Management

The Records Policy has been incorporated into the Data Protection Policy as it represents a key part of the overarching requirements of the GDPR. Changing the terminology of records to data should assist our change of perspective to meet the demands of the GDPR and privacy awareness in general.

The Minster Nursery & Infant School recognises that by efficiently managing its data, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the school. This constitutes *Privacy By Design* as proposed under GDPR rather than an additional layer on current practice. Under the legal requirements of the General Data Protection Regulation the school must be able to demonstrate that its policies cover how it gathers or receives information and how it is used, kept and disposed of. By maintaining evidence that we are protecting the legal and privacy rights of individuals (staff members, parents and children) and the interests of the school, we in turn demonstrate excellent performance and accountability. The school intends this document to provide the policy framework through which the effective data management can be achieved and audited.

The schools will take all practicable measures to ensure that personal data is securely held and access to it is controlled. The Act requires all organisations to have appropriate security to protect personal data against unlawful or unauthorised use or disclosure, and accidental loss, destruction or damage known as a ***Data Breach***.

This school recognises that the personal data it holds is valuable and must be managed properly as accidental loss, unlawful destruction or damage may cause distress to individuals concerned, bring disrepute on the school and result in official reprimand if not dealt with effectively, to a plan that includes containment and minimizing negative consequences of breaches when they occur.

Archiving: A small percentage of the school's records may be selected f or permanent preservation as part of the institution's archives and for historical research. To comply with GDPR legislation this data must be 'anonymised' or 'pseudonymised' so that no data can be associated with any individual. This will be achieved by allocating random codes to each data subject, which cannot be *backwardly-engineered* to reveal any identifiable data subject.

Retention & Destruction of Data

There is shredding available in the school. Where small amounts of paper-based data re produced, shredding should be done as required.

The school arranges regular onsite industrial shredding by a reputable company such as 'Shred-it'. If secure data has to be kept before shredding takes place, this must be kept secure prior to the bulk shredding process.

Non-compliance with this policy could have a significant effect on the efficient operation of the Schools and may result in financial and reputational loss and an inability to provide necessary services to our stakeholders.

Signed consent forms will be shredded at the same time as consent data is anonymized for that individual (*Data Subject)*.

Responsibilities

The school has a corporate responsibility as 'Data Controller' to maintain its records and record keeping systems in accordance with the General Data Protection Regulation (GDPR). The person with overall responsibility for this policy is the Head of the School. The Data Privacy Officer is the internal data lead (see appendix F – Provisional

Arrangements Re Data Protection Officer) and will ensure the school completes the tasks necessary to fulfill its requirements as the Data Controller, namely:

- Collect information to identify processing activities
- Analyse and check the compliance of processing activities
- Monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advising on data protection impact assessments, in addition to training staff and conducting internal audits.
- Inform, advise and issue recommendations to the controller or the processor
- Identify issues with the processing of third party processes)

Therefore the School Privacy Officer is the main internal contact with the external Data Protection Officer (DPO) Service. The DPO will make recommendations to the Head Teacher and Governors and will be continuously updated on Data Activity in the school, anything which warrants, or has warranted, contact with the Information Commissioner's Office (ICO) such as a Data Breach.
The Data Protection Officer Service will also give guidance to the about good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy by constant surveillance of the school's data handling processes.

Individual staff and employees must ensure that records for which they are responsible are kept secure, are accurate, and are maintained and disposed of in accordance with the school's records management guidelines.

Maintenance of Record Keeping Systems
Information gathered or processed by the school must be managed to the same standard of privacy and confidentiality regardless of the media in which it is stored.
It is important that filing information is properly resourced and is carried out on a regular basis. Information should not be recorded if it is unnecessary for any particular requirement of essential processing. This includes information where there may be some doubt such as a phone number that has not been written clearly. This must be verified before recording and would constitute a data breach if a recorded message was left on a wrong person's phone. *Extraneous information* must not be recorded namely; any data that is not essential to the fair processing of an individual's data. Removing, or altering, information from a file once a Freedom of Information or Subject Access Request (SAR) has been made, will be a criminal offence (unless it is has been part of normal processing).

Retention periods must be reviewed regularly against Retention Schedule (Appendix E). This has been assessed and will be regularly reviewed in reference to ICO https://ico.org.uk/for-organisations/guide-to-data-protection/principle-5-retention/

General Processing Procedure

- All managers and staff within the schools will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure
- Everyone managing and handling personal data must:
    - be appropriately trained to do so
    - be appropriately supervised
    - understand that they are contractually responsible for following good data protection practice as prescribed within this policy
- Methods of handling personal data are regularly assessed and evaluated and the evaluations are systematically recorded;
- Performance with handling personal data is regularly assessed and evaluated.

Data Sharing

- Data sharing is carried out in compliance with the GDPR, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

Subject Access Requests* or inquiries

- Anyone wanting to make enquiries about handling personal data, whether a member of staff or a member of the public, will be fully informed as to how to go about this.
  Queries about handling personal data are promptly and courteously dealt with. *See page 8 SARs

3rd Party Contractors

All contractors, consultants, partners or other servants or agents of the schools must: Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the schools, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between the schools and that individual, company, partner or firm;

- Allow and co-operate with data protection audits
- Indemnify the schools against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

All contractors who are users of personal data supplied by the schools will be required to confirm that they are complying with the requirements of the GDPR with regard to information supplied by the school. The school uses GDPRis software to corroborate company status re GDPR.

Implementation

The School Privacy Officer is the point of contact and data lead in the school.

The Data Protection Officer Service offers the supporting and detached role for the school, overseeing the data privacy culture, reporting any concerns to senior management and escalating broad or specific issues to, and maintains professional contact with, the external regulators such as the ICO. The **DPO** will offer guidance for best practice and will ensure all legal requirements of the school as 'The Processor' are done within the letter and the spirit of the law.

(see Appendix F – Provisional Decision on appointing a DPO Service).

Remote and Mobile Working

It is essential that access to all personal information is controlled. This can be done through basic precautions, such as locking the home office where practical or locking the computer's keyboard and making sure computers are not left in cars and hidden from view if necessary. Alternatively, or in addition, this can be done by password controls or User Login controls. Individual basic security agreement is signed for laptops and tablets leaving the school premises with a full list of such undertakings and an outline of procedures if an electronic item is lost and stolen.
It is essential that a crime number is gained straight away if needed and the loss is reported to the school to set in motion a Data breach notification.

Paper-based

It is a staff member's responsibility to ensure that the following points are adhered to at all times. When out of the office with school data:

- Paper based information and laptops should be kept safe, secure and close to hand when taken out of the office. Never leave them unattended. Particular care should be taken in public places.
- If files need to be taken off the premises they should be secured in the boot of a car or in lockable containers;
- Where personal information needs to be transported away from the schools this will be done on encrypted school laptops and encrypted memory sticks and not as paper documents.
- Information classified as personal data or sensitive personal data must not be stored on non-school owned devices (for example, a personal USB memory stick).
- When transporting paper copies of personal information away from the schools you must get permission from your line manager and must record what the information is, when you are taking it off site, the reason for doing so and the date when the information was returned.
- Removal of personal paper based information should only be for short periods and should be returned when the user is next in the office. If the user is subsequently off sick and the information not returned then this should be recorded.
- Paper based information should be kept confidential and secure when in transit and transported in a sealed file or envelope. This should indicate where it should be returned to if found.

Electronic

- Staff members must ensure that access/authentication passwords and personal identification numbers are kept in a separate location to the portable computer device at all times.
- Portable computer devices should be switched off, logged off, or the keyboard locked when left unattended, even if only for a few minutes.
- All data on portable computer devices must, where possible, encrypted. If this is not possible, then all personal or sensitive data held on the portable device must be encrypted. Teachers must use approved data memory sticks in order to access their files both at home and at school. Any data carried in this way must be encrypted using appropriate encryption software, e.g. Kingston Vault Privacy.
- When transferring paper-based or electronic data by car, ensure it is placed in the boot and is kept locked. Do not leave personal information or laptops in vehicles overnight.
- Personal information that is taken home should be stored in a locked drawer.
- Do not discuss confidential or sensitive work matters where you may be overheard by people who should not have access to the information e.g. in communal areas in the workplace or outside work.

- Return papers containing parent or carer personal information to the schools as soon as possible and file or dispose it securely in confidential waste bins.
- If paper based information or portable computer devices are lost or stolen then the loss must be reported to the user's line manager and Privacy Officer immediately and the process for reporting a Data Breach with all necessary recovery methods employed and recorded.
- After use, personal information on a USB memory stick must be securely deleted. It is unacceptable to continue to carry personal information on a portable electronic device beyond the required or necessary time.
- Any employee who chooses to undertake work using their own personal IT equipment is not permitted to hold any database, or carry out any processing of personal or sensitive personal data relating to the schools employees, parents, carers or stakeholders.
- Personal information should not be emailed to or auto forwarded to a private non-school email address. Secure email must be used to send personal information outside of the school network. Please also refer to the ***ICT Acceptable Usage Policy & Personal Commitment Statement.***

Good Office Practice

Paper-based

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment
- Files containing personal or sensitive information should not be left out on desks over night
- Do not leave documents containing personal information unclaimed on any printer.
- Do not leave documents containing personal information on your desk overnight or if you are away from your desk for long periods.
- Files should be disposed of safely in accordance with the Retention Schedule (Appendix E - Data Retention Schedule).
- Paper records containing personal information should be shredded using a cross-cutting shredder. Only non-confidential files can be bundled up and put in a skip or disposed of to the waste paper merchant. Loose papers should not be put in skips unless the skip has a lid. CD's/DVD's/Floppy disks should be cut into pieces. Audio/Video tapes and fax rolls should be dismantled and shredded. Confidential data awaiting bulk disposal with a biennial shred on location vehicle, should be kept under lock and key awaiting disposal.

Electronic

- Personal information held on computer systems should be adequately password protected. Information should never be left up on a screen if the computer is unattended
- All computer information is backed up daily using the London Grid for Learning/Atomwide 'Gridstore': a resilient, offsite backup service using the latest version of Attix 5 remote backup software
- Information contained in email, fax should be filed into the appropriate electronic or manual filing system once it has been dealt with.
- Sensitive personal information should not be sent by e-mail. The council Egress system should be used.
- Electronic data should be archived on electronic media and 'deleted' appropriately at the end of the retention period (see Appendix E)
- The discovery of incorrect recording of data about any person must be reported as a data breach. This includes, for example, a poorly filled in or unreadable form.
- Office workers must leave an entry blank rather than guess at details such as a phone number or address.
- Information on shared drives or electronic document management systems should only be stored in areas with appropriate access permissions, i.e., access is restricted to only those who have a need to view it
- Portable devices (laptops) should be secured (a locked drawer or Kensington Lock) particularly when left unattended and/or overnight within the schools.
- Any user accessing personal information must only use school-owned equipment
- Personal data should be stored on a shared drive or electronic document management systems wherever possible and not held on a portable computer device
- Personal information must only be disposed of in confidential waste bins
- Personal files must be sent by registered delivery, not by normal post
- Ensure that all postal and email addresses are checked to ensure safe dispatch of information. When sending personal information by post the envelope should clearly state '*Private – Contents for Addressee only'*.
- Ensure that when posting / emailing information that only the specific content required by the recipient is sent.

- Ensure that when sending confidential data within the school by email, the 'privacy' option is always used.

IT Infrastructure Security

- Access to the IT infrastructure, the physical locations and login access is limited to authorized staff members or approved 3rd party technicians.
  The school server is located in a secure location.
  There are nightly backups to the Gridstore which is a robust encrypted service provided LGfL/Atomwide.
  Sophos anti-virus and Malwarebytes malware protection is installed on the server and monitors all school and data traffic.
- The IT Officer has 2 level encryption to accessing online data
  - Atomwide as our main IT support organization have privileged access to the network and system. In turn, Octavo/LB Croydon have access to maintain the Capita SIMS managed information system (MIS).
  - **ICA Digital** which has the contract to maintain printers and the printer servers in the school and has automated services hosted on the school server.
- The SIMS MIS also provides direct export - import to these 3rd Party processors
  - ***ParentPay*** – Payment for lunches in the school
  - ***Lunch Hound*** which operated the till software for all children and staff

- Each of the above will be routinely examined for GDPR compliance and are be subject to a Data Protection Impact Assessment (DPIA).

- Reception and Nursery Teachers use one piece of software Tapestry that gathers cloud based data for assessing pupil progress and development. This keeps data in the cloud but within the EC. This is also subject to a risk assessment.

- Portable computing devices are provided to assist users to conduct official school business efficiently and effectively. This equipment, and any information stored on portable computing devices or data devices, such as USB sticks, must be securely encrypted and must be recognised as valuable organisational information assets and safeguarded appropriately.

Training and Awareness

The Senior Management Team will ensure that employees responsible for handling personal information are appropriately trained and have experience of Information security and that all officers understand the need for compliance with information security (see ***General Processing – Page 11***)

A training programme is established to ensure that all officers are aware of their responsibilities for information security and a record is kept of this provision.

Information security is part of the induction process for all school employees and members.

Mandatory training for all staff in key areas (data protection, information security, records management, incident / breach reporting and requests for personal data);

There is specialised training for some roles where data handling is prevalent; annually refreshed training; responsibilities for recording and monitoring of training should be included.

Notification to the Information Commissioner's Office

The Minster Nursery & Infant School is the Data Controller under the law and is registered with the Information Commissioner's Office.

The Privacy Officer is responsible for notifying and updating the Information Commissioner's Office of changes to annual renewal and also immediately with regard to Data breaches. Any individual, employee or otherwise, can also contact the ICO with his or her concerns. Contact information will be publicized in the school.

Financial Penalties, Criminal Offence & Data Breaches

There are serious repercussions under the law for data breaches which are not properly dealt with or if there is poor liaison or follow up with the ICO. This is seen as a corporate responsibility. The School will respond pro-actively to data breaches, documenting, the breach, the cause or causes, the procedures we have in place to mitigate negative effects and how we subsequently recover from such a breach and improve practice where necessary. This process requires recording and making available on request for scrutiny and external verification.

The ICO regards a complete absence of data breaches as potentially suspicious and it is expected that breaches will occur.

Individuals may be in breach of their terms of employment if there is a flagrant disregard of a signed agreement to endeavor to protect privacy or causing a breach that jeopardises employees, parents, carers or children's privacy. Neglect of professional obligations may be cause for disciplinary action which could result in dismissal from the schools' employment.

Disciplinary action would only be one possible part of the school's corporate response.

In the event of a data breach, the school as ***Data Controller***

- has 72 hours to inform the ICO
- Must have a good idea of the potential detrimental effects on individuals
- Must be able to demonstrate that the school is working within a procedure of containment and recovery
- If the incident is deemed 'high risk' all individuals whose personal data and therefore privacy has been jeopardized must be informed

- Detrimental Effects on Individuals may include:
  - Discrimination
  - Damage to reputation
  - Financial loss
  - Loss of confidentiality
  - Any other significant economic or social disadvantage

If you require any further assistance please contact:

The Data Protection Officer
Democratic and Legal Services
Chief Executive's Office
London Borough of Croydon
Bernard Weatherill House,
8 Mint Walk,
Croydon,
CR0 1EA

Policy Compliance

All employees are required to have read and understood this policy which will be issued to new members of staff and renewed by arrangement. This will also be available on the school website.

If any employee is found to have breached this policy, they may be subject to the schools disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

The school will also be obliged to notify the Information Commissioners Office and issue a Data Breach Notification. This must occur within 72 hours of the incident occurring with a full appraisal of what took place and what has been done to mitigate the effects of the breach.

If you do not understand the implications of this policy or how it may apply to you, seek advice from the Privacy Officer.

Policy Governance

The following table identifies who within the schools is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

Responsible – the person(s) responsible for developing and implementing the policy.
Accountable – the person who has ultimate accountability and authority for the policy.
Consulted – the person(s) or groups to be consulted prior to final policy implementation or amendment.
Informed – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	The School Lead Privacy Officer, Governing Body
Accountable	Head Teacher
Consulted	Senior Leadership Team
Informed	All employees

Review and Revision

It is expected that this policy and related procedures will have frequent updates over the next few years. Therefore the policy will initially be reviewed more regularly than every 12 months. It will be amended to maintain its relevance. Further reviews will be undertaken to reflect changes in legislation or standards.

Policy review will be undertaken by the Governing Bodies of The Minster Nursery & Infant School.

Version control			
Version Number	**Date issued**	**Prepared by**	**Update information**
v1.0	26.07.18	D.W.	First published version
v1.1	05.12.18	D.W,	Amended after ICO and DPO recommendations

Appendix

GDPR legislation requires an increase of forms, record keeping and centralized accessible locations for monitoring. Here are some but not all of key documents pertinent to, and mentioned in, the policy document.

Appendix A – Privacy Notice – Parents, Carers & Pupils
Appendix B – Privacy Notice – Employee Workforce
Appendix C – Photography & Film Consent Form
Appendix D – Photography & Film Alteration or Consent Withdrawal Form
Appendix E – Data Retention Schedule
Appendix F – DPO Service – South Croydon Cluster
Appendix G – Electronic & Digital Security
Appendix H – Data Risk Schedule
Appendix I – DPIA (Data Protection Impact Assessment) Proforma
Appendix J – Data Breach Procedure & Report Form
Appendix L – Tapestry Consent Form
Appendix M – Subject Access Request Form

An up-to-date version of this policy can be found at http://minsterinfants.co.uk/privacy/

This version: Sunday, September 22, 2019
Located at O:\GDPR\Policies\Dec_2018 Policy Review