Bedford Nursery Schools Federation

Data Protection Policy

Approved by governors: Dec-19

Chair of Governors: Jane Walker

Reviewed: Dec-22

Next Review date: Dec-24

General Statement

Bedford Nursery Schools Federation recognises The General Data Protection Regulations (GDPR) which came into force 25th May 2018. It is concerned with the rights of individuals within it and the right to challenge the accuracy of data held. The terms of the Act relate to data held in any form, including written notes and records, not just electronic data.

Bedford Nursery Schools Federation (All references to Bedford Nursery Schools Federation in this document also apply to the business of Peter Pan Training Partnership) is committed to conducting its business in accordance with Data Protection laws and standards in line with the highest standards of ethical conduct. The schools leadership team is fully committed to ensuring continued and effective implementation of this policy, and expects all its employees and third parties to share this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action.

This policy applies to personal information held and processed by Bedford Nursery Schools Federation, and sets out its duties under the GDPR Regulations. The policy provides guidance on the processing, retention, security and disposal of all personal data held by Bedford Nursery Schools Federation. The policy applies to all employees, governors, contractors, agents, representative's, volunteers and temporary staff working for or on behalf of the school.

Bedford Nursery Schools Federation is required to process personal data regarding members of staff, volunteers, applicants, parents, pupils, their siblings, and customers as part of our day to day operations and shall ensure that all reasonable steps are taken to comply with this policy and the principles of the GDPR Regulations and Data Protection Guidance.

The school aims to have a transparent system for holding and processing personal data. Any reference to personal data within this policy includes reference to sensitive personal data. Processing may include obtaining, recording, and handling, disclosing, destroying or otherwise using data.

An individual is entitled to request access to information relating to their personal data held on a relevant filing system by the school. A relevant filing system is any paper filing system or manual filing system which is structured so that information about an individual is readily accessible. Personal data can be held in any format (electronic, paper-based and photographic) from which the individual's data can be readily extracted. In this policy any reference made to pupils includes current, past and prospective pupils.

General Data Protection Regulations

Bedford Nursery Schools Federation has a responsibility to comply with GDPR regulations. The GDPR regulations apply to all data that is both personal and sensitive.

Personal data means data relating to a living individual who can be identified from that data. The school may process a wide range of personal data of pupils, their parents or guardians and staff, as part of our operations. To qualify as personal data, the data must allow you to identify and give information relating to a data subject. Personal data includes facts and any expression of opinion about an individual. Examples of personal data are: names and addresses, bank details, academic, disciplinary, admission and attendance records; references; academic data.

Current data protection legislation does not apply to access to information about deceased individuals. However, the duty of confidentiality may continue after death.

Sensitive personal data is defined as information in respect of racial or ethnic origin, political opinions, religious beliefs or beliefs of a similar nature, membership of a trade union, physical or mental health, sexual life, criminal conviction and alleged offences. Sensitive personal data can only be processed under strict conditions, including a condition requiring consent of the person concerned to such processing.

Each entity of Bedford Nursery Schools Federation will adopt physical, technical, and organisation measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks which it may be exposed to by virtue of human action or the physical or natural environment.

The minimum set of security measures to be adopted by each of Bedford Nursery Schools Federation is provided in the 'Record Management and Information Security Policy'.

Policy Dissemination and Enforcement

The Senior Leadership Team must ensure that all employees of Bedford Nursery Schools Federation that are responsible for the processing of personal data are aware and comply with the contents of this policy.

The Principles

Data protection legislation stipulates that anyone processing personal data must comply with principles of good practice; these principles are legally enforceable. The 8 principles require that personal data:

1. Shall be processed fairly and lawfully and transparently;

   The collection and disclosure of data is subject to scrutiny and is only lawful if it meets at least one of the following criteria:

   a) With the consent of the data subject; or
   b) In performance of a contract (for example to process an application as part of the admission process); or,
   c) If there is a legal obligation; or
   d) For the protection of the vital interests of the individual (for example to prevent injury or other damage to the health of the data subject), or,
   e) The processing is necessary for you to perform a task in the public interest and the task has a clear basis in law, or,
   f) In the legitimate interest of the data controller, unless it is prejudicial to the interests of the individuals data.

   Personal data must meet all of the following criteria in order to be processed 'fairly':

   a) Data will only be collected from persons who have the authority to disclose it. If personal information is collected from a third party, the data subject will be informed if the 'use' of the information.
   b) Subjects will not be deceived or misled in any matter related to the use of personal data.

In addition to the requirements outlined above, sensitive (special) personal data may only be processed if it also meets at least one of the following criteria:

a) The data subject has given explicit consent
b) It is necessary to meet requirements of employment law
c) It is necessary to protect the vital interests (i.e. if it is a matter of life or death situation) of the subject or another person
d) Processing carried out in course of legitimate activities with appropriate safeguards.
e) The data subject has already manifestly made the information public
f) It is necessary for legal proceedings, obtaining legal advice or defending legal rights
g) It is necessary for the carrying out of official or statutory functions (in the public Interest)
h) It is necessary for purpose of preventative or occupational medicine.
i) It is necessary for public health
j) It is necessary for archiving purposes in the public interest or historic/statistical research purposes order to comply State Law.

2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;

   Data will not be further processed in any manner incompatible with the initial specified purpose or those purposes for which it was obtained. To satisfy the first principle (fair processing) the data subject(s) must not have been misled or deceived as to the reason(s) for processing.

3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;

   Personal information, which is not necessary for the intended processing, must not be acquired, i.e personal information cannot be collected just because it may be useful

4. Shall be accurate and where necessary, kept up to date.

5. Shall not be kept for longer than is necessary for that purpose or those purposes;
   a) Any legal requirements
   b) The length of any appeals procedure relating to this information
   c) The number of time in the last two years that a particular type of record has been accessed

6. Data must be processed in line with individual's rights

   This is strongly linked to the first principle of fair and lawful processing. Data subjects have the right to know details of the processing and the right of access to personal information.
   A data subject has the right to object to data processing relating to them which is likely to cause damage or distress to that data subject of another person. There are a number of provisos to this right, in particular;
   a) The damage or distress must result from unwarranted processing, or
   b) The data subject must not have given consent to the processing, or
   c) The processing is not necessary for the purposes of fulfilling a contract with the data subject; or for fulfilling a legal obligation of Bedford Nursery Schools Federation, or for protecting the data subject's vital interests

   In addition the Act gives data subjects the right to object to processing used for the purpose of direct marketing and/or wholly automated decision making.
   Data subjects have the right to have inaccurate data amended and to block future processing in cases of unlawful/unfair processing. Data subjects must formally request their rights in writing and their rights are enforceable by the courts.

7. Data must be processed in a secure manner i.e. protected by an appropriate degree of security;

8. Data shall not be transferred outside of the UK unless that country or territory ensures an adequate level of protection

   If the data is to be transferred to a country or territory that does not have adequate protection then at least one of the following conditions must be met:
   a) The data subject has given consent
   b) It is necessary for the performance of a contract with the data subject
   c) It is necessary for the performance of a contract that is in the interests of the data subject
   d) The transfer is necessary for reasons of substantial public interest
   e) The personal data is already on a public register
   f) The transfer is necessary to pursue legal proceedings, legal advice or defending legal rights
   g) It is in the vital interest of the data subject
   h) The Information Commissioner has approved the transfer on the grounds that it safeguards the rights and freedoms of the data subject

In addition, it must take into account UK rules on transferring data outwards from the UK to the EU (including the EEA) and the rest of the world and the impact of EU transfer rules on those sending you personal data from outside the UK (including from the EEA) into the UK

In both cases, you can transfer personal data if it is covered by an adequacy decision, an appropriate safeguard, or an exception.

In addition, the data shall be processed in accordance with the rights of data subjects.

Responsibilities under the Data Protection Act (DPA)

Bedford Nursery Schools Federation as a body is the data controller under the DPA. Bedford Nursery Schools Federation will act as a data processor of personal data for the data held in line with the purposes notified to the Information Commissioner.
The Governing Body is responsible for the school's compliance with the Data Protection Act and ensuring that other school policies and practices are consistent with this policy. The Governing Body are responsible for ensuring that all staff are aware of their responsibilities under the act and appropriate training is put in place.
The Governing Body will nominate **ROBIN THOMAS (GOVERNOR –Chair of Finance Committee**) to act as their registered Data Protection Officer **(DPO)**.
Compliance with the GDPR is the responsibility of all members of the school.

Notification

Notification is the responsibility of the Data Protection Officer. Details of the school's notifications will be published on the Information Commissioner's Office **(ICO)** website. Anyone who is, or intends processing data for the purposes not included in the school's notification should seek advice from the DPO.
The Digital Economy Act 2017 requires every data controller who is processing personal data, to notify and renew their notification to the ICO on an annual basis. Failure to do so is a criminal offence. The ICO maintains a public register of data controllers, in which the school must be registered. The school will review the Data Protection Register annually, prior to renewing its notification to the Information Commissioner.

Processing Personal Data

Processing of personal data includes obtaining, holding, recording, adding, deleting, augmenting, disclosing, destroying, printing or otherwise using data. Processing also includes transferring data to 3rd parties.
Bedford Nursery Schools Federation will make sure that all Third Parties engaged to process personal data on their behalf are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all Third Parties, whether companies or individuals, prior to granting them access to Personal data controlled by Bedford Nursery Schools Federation. All third parties will be contacted prior to sharing of data to ensure GDPR compliance.
Consent may be require for the processing of personal data unless the processing is necessary for the school to undertake their obligations to pupils and their parents or guardians. Personal data, unless otherwise exempt from restrictions on processing under the DPA, will only be disclosed to third parties under the terms of this policy or otherwise with the consent of the appropriate individual.
The rights in relation to personal data set out under the DPA are those of the individual to whom the data relates. The school will rely on parental or guardian consent to process data relating to pupils, and those with parental responsibility are entitled to receive relevant information concerning the child.

Data Protection by Design

To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes (with new technology), and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing.

Each entity must ensure that a Data Protection Impact Assessment (DPIA) is conducted, in cooperation with the Data Protection Administrator, for all new and/or revised systems or processes for which it has responsibility and risks identified and procedure to mitigate risks should be approved by the Senior Leadership team.

Collection of data

Personal data should be collected only from the Data subject unless one of the following apply:

a) The nature of the business purposes necessitates collection of Personal data from other persons or bodies
b) The collection must be carried out under emergency circumstance in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person

If personal data is collected from someone other than the Data Subject, the Data Subject must be informed of the collection unless one of the following apply:

a) The Data Subject has received the required information by other means
b) The information must remain confidential due to a professional secrecy obligation
c) A national law expressly provides for the collection, processing or transfer of the personal data

Use of personal data

GDPR requires that the personal data held about pupils must only be used for specific purposes allowed by the law. The school holds personal data on its pupils, including; contact details, assessment/examination results, attendance information, behaviour, both positive and negative and characteristics such as ethnic group, special educational needs, any relevant medical information, and photographs.
The data is used in order to support the education of the pupils, to report in their progress, their parents or guardians for fundraising, marketing, and to maintain relationships with pupils of the school.
In particular, the school may:

a) Make use of photographs of pupils externally for marketing purposes (brochures), on the closed Facebook group, or on its website.
b) Make use of photographs internally for school displays, children's Learning Journeys or for the purpose of staff training
c) Make personal data, including sensitive personal data, available to staff for planning curricular activities; (medical conditions/medication and SEN)
d) Sending a final report to the primary school that the children will be attending.
e) Sending of any safeguarding paperwork to the next school or setting (statutory).

The school will ensure that all data subjects have read and signed the schools consent section which form part of the initial school application form

If there are circumstances in which personal data may be further processed for purposes that go beyond the original purposes for which the personal data was collected then guidance and approval must be obtained from the Headteacher before any such processing may continue taking into account the data protection principles

Special (Sensitive) Categories of Data

Bedford Nursery Schools Federation will only process Special Categories of Data (also known as sensitive data) where it meets one of the criteria listed in the data protection principles, outlined earlier in this policy.

In any situation where Special Categories of Data are to be processed, prior to approval must be obtained from the Data Protection Administrator and the basis for the processing clearly recorded with the Personal data in question.

Children's Data

Children are unable to consent to the processing of Personal data for information society services. Consent must be sort from the person who holds parental responsibility over the child. However, it should be noted that where processing is lawful under other grounds, consent need not be obtained by the holder of parental responsibility.

Accuracy of personal data

The school will endeavour to ensure that all personal data held in relation to an individual is accurate. Individuals must notify the school of any changes to information that is held about them. The school will proactively ensure that data checking processes are carried out to ensure accuracy of the data held. Reminders are sent out in newsletters and social media to ensure parents update regulary. An individual has the right to request that inaccurate information about them is erased or corrected.
Bedford Nursery Schools Federation will adopt the measure below to ensure data quality:

a) Correcting Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification
b) Keeping Personal data only for the period necessary to satisfy the permitted uses or applicable statutory retention period
c) The removal of Personal data if in violation of any of the Data Protection principles or if the Personal data is no longer required
d) Restriction, rather than deletion of Personal data, insofar as:

- A law prohibits erasure
- Erasure would impair legitimate interest of the Data Subject
- The Data Subject disputes that their Personal data is correct and it cannot be clearly ascertained whether their information is correct or incorrect

Exemptions which all disclose of personal data to third parties

There are a number of exemptions in the GDPR which allow disclosure of personal data to third parties, and the processing of personal data by the school and its employees, which would otherwise be prohibited under the GDPR. The majority of these exemptions only allow disclosure and processing of personal data where specific conditions are met, namely;

a) The data subjects have given their consent;
b) To safeguard national security;
c) For the prevention and detection of crime;
d) To prevent serious harm to the data subject or a third party;
e) For the assessment of any tax or duty;
f) Where it is necessary to exercise a right or obligation conferred or imposed by law upon the school (other than an obligation imposed by contract);
g) For the purposes of, or in connection with, legal proceeding (including prospective legal proceedings);
h) For the purposes of obtaining legal advice;

Disclosure of personal data to third parties

The school may at times receive requests from third parties (i.e. those other than the data subject, and employees of the school) to disclose personal data it holds about its pupils, their parents or guardians. This information will not generally be disclosed unless one of the specific exemptions under the GDPR which allow disclosures applies; or where necessary for the legitimate interests of the individual concerned or the school.
The following are the most usual reasons that the school may have for passing personal data to third parties:

a) Give information relating to outstanding fees or payment history to any educational institute which is it proposed that the pupil may attend; please note that the school reserves the right to share personal information with third party credit reference agencies if it is considered by the school to be necessary;
b) Disclose details of a pupils medical condition where it is in the pupils interest to do so, for example for medical advice, insurance purposes or to organisers of school trips;
c) Provide information to another educational establishment to which a pupil is attending or is transferring to; and
d) Disclose information to social services/health team when requested
e) Provide information with local authority for funding /EYPP
f) Provide the relevant information to the Government Department eg. DfES, Ofsted

The Department for Education uses information about pupils for statistical purposes, to evaluate and develop educational policy and practices and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual pupils cannot be identified from them.
Any wish to limit or object to any use of personal data by third parties, except as stated above, should be notified in writing to the school designated DPO.
Where the school receives a disclosure request from a third party it will take reasonable steps to verify the identity of the third party before making any disclosure. When members of staff receive enquiries from third parties for personal data, the enquirer should be asked why the information is required. If consent to the disclosure has not been given (and an exception does not apply) then the request should be declined. In normal circumstance information should not be disclosed over the phone to third parties. In most circumstances third parties should be asked to provide documentary evidence to support data requests.

Data Transfer

The entities of Bedford Nursery Schools Federation may transfer personal data to internal or third parties located in another country where the country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant Data Subjects.
Where transfers need to be made to a country lacking adequate level of legal protection (i.e third world countries), they must be made in compliance with an approved transfer mechanism.
Entities of Bedford Nursery Schools Federation may only transfer personal data where one of the transfer scenarios listed below applies:

a) The Data Subject has given consent to the proposed transfer
b) The transfer is necessary for the performance of a contract with the Data Subject
c) The transfer is necessary for the implementation of pre-contractual measures taken in response to the Data Subjects request
d) The transfer is necessary for the conclusion or performance of a contract concluded with a Third Party in the interest of the Data Subject
e) The transfer is legally required on important public interest grounds
f) The transfer is necessary for the establishment, exercise or defence of legal claims

Subject Access Requests

Rights of access by data subjects to their personal data (Subject Access Requests)

Under GDPR, individuals have the right of access to their personal data held by the school. Generally in the case of pupils under the age of 12 years, the person with parental responsibility may exercise this right on their behalf. This is known as a Subject Access Request. A request in writing will be accepted as long as satisfactory identification is given and the information request is clear, not excessive. Where the pupil and parents are known to the school further identification will not be required. In other cases it is expected that picture ID, such as a passport or driving licence would be required.

There will be no charge for the Subject Access request usually, however, we would charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive and also in the case where there are requests for further copies of the same information.

Responding to requests for access to records (Subject Access Requests)

The school will send a written response to the applicant acknowledging receipt of the request. The DPO will manage the response to the applicant. The DPO will also maintain a SAR process sheet (see Appendix 1). The purpose of the process sheet is to clarify the request, ensure the request is scrutinised, monitor request deadlines and record contact with and information sent to the applicant. It will also record decisions taken with regard to the application.
The Head teacher must authorise the applicants request before any information is disclosed.
The school will consult with its HR services if there is any query over the information that has been requested. If the applicant's request for access is granted, the DPO requires such access to be given within 1 month days of the written request being received, provided that the school has received sufficient information to enable it to identify the individual who is seeking access and the school has received sufficient information to enable it to access the information requested

Where the conditions set out above are fulfilled, in responding to the request, the school must give a description of the personal data that is being processed, the purposes for which the personal data is being processed, and the persons to whom the personal data has been disclosed too. The school should agree a secure method of releasing the information to the applicant.

Data subjects are not entitled to information where exemptions to the right of access apply. In these circumstances, the school must only give a notification to the data subject, that no information has been identified which is required to be supplied under the DPA regulations.

Exemptions to access by data subjects

Confidential references given, or to be given by the school are exempt from access. The school will therefore treat as exempt any reference given by them for the purpose of education, training, employment or prospective education, training, employment of any staff member or pupil.
It should be noted that confidential references received from other parties may also be exempt from disclosure. However, such a reference can be disclosed if the disclosure will not identify the source of the reference or where the referee has given their consent, or where disclosure is reasonable in all the circumstances.
Data covered by Legal Privilege is also exempt i.e. where it may be necessary to take legal advice regarding a data subject; this information is exempt to any SAR.

Retention of data

The school will not keep pupil and related data for longer than necessary. The school will use the retention periods recommended in the Information Management Toolkit and will dispose of records securely after the recommended time. The school has a written Record Management and Information Security Policy which sets out the schools records management protocols.

CCTV Code of practice

The Data Protection Act requires a systematic legal control of the CCTV surveillance through the Code of Practice (October 2001). Bedford Nursery Schools Federation to no longer operates any CCTV surveillance and has no stored CCTV images. There are CCTV cameras on the Peter Pan Nursery School site but these are not operational.

Complaints Handling

Data Subjects with a complaint about the processing of their personal data, should put forward the matter in writing to Data Protection Officer .An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Data Protection Officer will inform the Data Subject of the progress and outcome of the complaint in a reasonable timeframe.
If the issue cannot be resolved through consultation between the Data Subject and the Data Protection Officer, then the Data Subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Data Protection Authority within the applicable jurisdiction.

Data Breach Reporting

Any individual who suspects that a personal data breach has occurred due to the theft or exposure of personal data must immediately notify the Data Protection Administrator providing a description of what has occurred. Please refer to Appendix 2, 2a & 2b for details of procedure to follow in regards to a data breach.

Audit and Review of Policy

This policy will be reviewed annually in conjunction with an annual compliance audit (Appendix 3). Each audit will, as a minimum, assess:

a) Compliance with Policy in relation to the protection of Personal data, including:
b) The assignment of responsibilities
c) Raising awareness
d) Training of Employees
e) The effectiveness of Data Protection related to operational practices, including:
    - Data Subject rights
    - Personal data transfers
    - Personal data incident management
    - Personal data complaints handling
    - The level of understanding of Data Protection policies and Privacy notices
    - The currency of Data Protection policies and Privacy Notices
    - The accuracy of Personal data being stored
    - The conformity of Data Processor activities
    - The adequacy of procedures for redressing poor compliance and Personal data Breaches

The Business Manager/Office Manager in cooperation with key stakeholders will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame. Any major deficiencies identified will be reported to and monitored by Bedford Nursery Schools Federation Leadership Team.

Changes to the policy will come into force once the policy has been agreed by the school Governing Body.

Appendix 1

Subject Access Request Process

Name of Data Subject :
Type of Data subject: (current or former- employee/volunteer/job applicant/pupil/parent of pupil)
Name of Data Applicant (if different from Data Subject- would be parents/carers):
Contact Details of Data Applicant/ Data Subject:
Date of WRITTEN data request: (can include emails)
Deadline of data request response: (1 calendar month of request)

Data Request specifics:

Subject Access Request Checklist

	Checked?	Comments
Has Head teacher Authorised SAR?		
Check If data applicant/data subject known, Has relevant ID been seen if not known? (passport/driving license)		
Check Parental responsibility (if applicable)		
Confirmed method of delivery of request (hand delivered/secure email/special delivery?)		
Does data request need clarification? Do we need to consult with HR or other LA teams?		
Does any of the data requested exempt from being supplied (check ICO guidance)?		
Have we confirmed receipt of request to applicant? (in writing)		

Is the data request excessive or a repeat of a past request from same applicant? If so follow ICO guidance (could charge an admin fee or refuse to supply same information again).		
Ensure data looked at from paper and electronic sources		
Check if data found of data subject also has data about other data subjects, all references to these data subjects must be redacted unless prior consent gained or is reasonable to provide their information without consent.		

Method of extraction of data:
Response to the request:
What personal data is being processed?

What is the purpose of the personal data being processed?
Who has this personal data has been shared with?

Appendix 2

Data Protection - Data Breach Procedure

Policy Statement

Bedford Nursery Schools Federation holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by the school and all school staff, Governors, volunteers and contractors, referred to herein after as 'staff'.

Purpose

This breach procedure sets out the course of action to be followed by all staff if a data protection breach takes place.

Legal Context

Article 33 of the General Data Protection Regulations
Notification of a personal data breach to the supervisory authority

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

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
(c) describe the likely consequences of the personal data breach;
(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

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

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

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

1. The person who discovers/receives a report of a breach must inform the Head Teacher or, in their absence, either the Deputy Head Teacher and/or the School's Data Protection Officer (DPO). If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

2. The Head Teacher/DPO (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.

3. The Head Teacher/DPO (or nominated representative) must inform the Chair of Governors as soon as possible. As a registered Data Controller, it is the school's responsibility to take the appropriate action and conduct any investigation.

4. The Head Teacher/DPO (or nominated representative) must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the School's legal support should be obtained.

5. The Head Teacher/DPO (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

a. Attempting to recover lost equipment.

b. Contacting the IT support company, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned. Consideration should be given to a global email to all school staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual, making the enquiry, back. Whatever the outcome of the call, it should be reported immediately to the Head Teacher/DPO (or nominated representative).

c. Contacting the Bedford Borough Council's Press Office, so that they can be prepared to handle any press enquiries.

d. The use of back-ups to restore lost/damaged/stolen data.

e. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

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

Investigation

In most cases, the next stage would be for the Head Teacher/DPO (or nominated representative) to fully investigate the breach. The Head Teacher/DPO (or nominated representative) should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

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

A clear record should be made of the nature of the breach and the actions taken to mitigate it, this will be recorded on the Data Breach Form (Appendix 2a). The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The Head Teacher/DPO (or nominated representative) should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case by case basis.

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

			Data Breach No	

done to mitigate the risks posed by the breach

Review and Evaluation
Once the initial aftermath of the breach is over, the Head Teacher/DPO (or nominated representative) should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Senior Management Team and Full Governors meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources or Internal Audit for advice and guidance. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

A Data Security Breach log is filled in for every breach- **see appendix 2b.**

Implementation
The Head Teacher/DPO should ensure that staff are aware of the School's Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the School's Data Protection policy and associated procedures, they should discuss this with their line manager, DPO or the Head Teacher.

Appendix 2a

			Severity of breach	High	Med	Low
	Report prepared by:					
	Date completed:		**Completed within 3 days of incident report date**		**Yes**	**No**
1	**Date incident reported, by whom and how**					
2	**Summary of the incident and circumstances**		*When, what, who, summary of incident etc.*			
3	**Type and amount of personal data**		*Document names/personal data items/ description of information about the individual(s) e.g.; medical conditions; address and contact details etc.*			
4	**Actions taken by individual on discovery of breach**					
5	**Initial actions taken to respond to the breach**		*What immediate steps have been taken to contain the breach? Or recover data loss?*			
6	**Risk assessment of incident**		*Has a risk assessment been taken and logged in DPIA form? Has level of risk been addressed?*			
7	**Details of notification to affected data subject(s)/Governors/ ICO/third parties**		*Who has been notified; when and why.*			
8	**Procedures / instructions in place to minimise risks to security of data**		*What remedial actions put in place to prevent reoccurrence? i.e. communications to staff; changes to technical procedures etc.*			
9	**Details of longer term procedural changes to reduce risks of future data breaches**		*Review of training; changes in procedures and policy etc.*			
10	**Conclusion**		*Was it a serious/minor breach? Is it likely to happen again?*			

Data Breach Report Form-Bedford Nursery Schools Federation

Appendix 3

Description	Current Situation	Status	Action(s)	Owner	Deadline	Completed
Staff/ Pupil Records						
Student data is kept in accordance with the data retention policy						
Staff data is kept in accordance with the data retention policy						
Expired records are disposed of safely and securely by named individuals						
All forms used to collect data are identified						
All forms used to collect data include the standard data protection disclaimer						
The Pupil Data collection Sheet is sent out annually to collect and refresh pupil data						
All electronic databases in use, including the users who can access them can be identified (RM Finance, Integris,Synergy)						
Access to all electronic databases is secured by individual usernames and password (RM Finance, Integris Synergy)						
All paper record systems in use, for staff or pupils are identified						
All paper record systems are secured in accordance with Data Protection Guidance						
Staff with access to staff records is documented, controlled and regularly reviewed						
The school Parental Data Protection, Media and Home School agreement is being used						
The accident book and logs are being used and are kept in accordance with the school retention policy						
All pupils whose parents have opted for them not to have photographs used are clearly identified and this information is						

accessible to all staff						
Procedures						
All third party organisations offering a service on the school premises, including the data they collect are identified. Any third party using cloud based services must confirm that they are complaint (Redstor)						
All Service Level Agreements with third party organisations are reviewed and compliance established						
The contact details of parents are not distributed to other parents, for legitimate activities, unless a signed parental Consent Form is received by the school						
A Subject Access Request file is in place						
The Subject Access Request process has been tested.						
Staff Training						
Staff are made aware of the Data Protection Policy and sign to confirm they have read and understand the policy						
Staff are made aware of the schools ICT Acceptable Use Policy and sign to confirm they have read and understand the policy						
Staff have received appropriate training and guidance on Data Protection processed and practices						
Staff have been issued with the do and don't list						
Staff are made aware of how to report data breaches						

Audit completed by (Please Print) ……..
Signed: …….
Position: …….
Date: ……