St John's Community Primary School and Nursery

Data Protection Policy

[Version 2018 v1.3]

If you are reading a printed version of this document you should check the Information Management pages on [the school network] to ensure that you have the most up-to-date version.

If you would like to discuss anything in this privacy notice, please contact:

Data Protection Officer: **Stuart Lee**

Telephone: 0800 0862018

Email: dpo@dataprotection.education

If you would like a copy of any documentation please contact the school office:

Tel: 01603 782520

Email: office@hoveton-st-johns.norfolk.sch.uk

Document version control

Version	Author	Date	Approved by	Effective from
1.1	DPE - JE	1/5/2018		
1.2	DPE - TK	2/5/2018		
1.3	SJP – EW	7.5.18		

Contents

Document version control 2
Contents 3
Introduction 4
Scope 4
Definitions 4
Commitment to GDPR and Data Protection by Design 7
Data Principles 7
Data Subject's Rights 8
Lawful processing 8
Information Commissioner's Office 9
Data Sharing 9
Data Breaches 10
Subject Access Requests 11
Dealing with a subject access request (SAR) 12
Data Protection Officer 13
Data Security 14
Photography and Videos 15
CCTV 15
Retention Policy 15
Training 16

Introduction

Scope

This policy reflects The Organisations commitment to the General Data Protection Regulation (GDPR) and the expected provision of the 2018 Data Protection Act, as of May 1st 2018 passing through parliament as the Data Protection Bill.

This policy covers the processing of personal data wholly or partly by automated means and the processing (other than by automated means) of personal data which form part of a filing system or are intended to form part of a filing system.

Definitions

As defined by the GDPR:

- **personal data** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is a person 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 by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- **processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, 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;
- **restriction of processing** means the marking of stored personal data with the aim of limiting their processing in the future;
- **profiling** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
- **pseudonymisation** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

- **filing system** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
- **controller** means 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- **processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- **recipient** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
- **third party** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
- **consent** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- **personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- **genetic data** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
- **biometric data** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
- **data concerning health** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
- **enterprise** means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;
- **supervisory authority** means an independent public authority which is established by a Member State pursuant to Article 51 of the GDPR;
- **cross-border processing** means either:

- processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
- processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State;
- **relevant and reasoned objection** means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;
- **information society service** means any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services;
- **international organisation** means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;
- **special categories** of personal data means personal data:
    - revealing racial or ethnic origin,
    - revealing political opinions,
    - revealing religious or philosophical beliefs or trade union membership,
    - the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person,
    - data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited;
- **data breach**: an incident or event in which personal and/or confidential data:
    - has potentially been viewed or used by an individual unauthorised to do so;
    - has had its integrity compromised;
    - is lost or is unavailable for a significant period.

Commitment to GDPR and Data Protection by Design

This policy sets out The Organisation's commitment to GDPR and the implementation of a data protection by design approach. The Organisation will refer to documents and guidance from the Information Commissioner's Office and the Department for Education in relation to GDPR and data processing. This includes ensuring by May 25th 2018 and beyond:

- Creation and maintenance of a data protection working group;
- Assigning responsibility to an individual within The Organisation;
- Assigning a Data Protection Officer;
- Development and maintenance of a GDPR project;
- Ensuring that all staff are trained in data protection and take responsibility for the collection, processing, storage and destruction of data;
- A lawful basis for processing is documented for all processing activity;
- Principles relating to processing of personal data are adhered to;
- The rights of data subjects are respected;
- Risks to the rights of data subjects are assessed and mitigated for all large-scale and new processing;
- Regular independent reviews of processing activity and processing documentation are carried out;
- Organisational and technical measures are implemented to protect data;
- Data breaches impacting on the rights and freedoms of data subjects will be reported to the ICO.

Data Principles

The Organisation is committed to the principles relating to processing of personal data, in that personal data will be:

- **processed lawfully, fairly and in a transparent manner** in relation to the data subject;
- **collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes;
- **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed;
- **accurate and, where necessary, kept up to date;**
- **kept in a form which permits identification of data subjects for no longer than is necessary**;

- **processed in a manner that ensures appropriate security of the personal data**.

Data Subject's Rights

The Organisation supports the rights of data subjects (or the parents/carers of data subjects where data subjects are not able to demonstrate the capacity to understand their rights) in relation to data that is processed or stored about them, as follows:

- Right to fair and transparent processing;
- Right of access;
- Right of rectification;
- Right to erasure (the "right to be forgotten");
- The right to restrict processing;
- Right to be notified of erasure, rectification or restriction;
- Right of data portability;
- Right to object to processing;
- Right to object to processing for the purposes of direct marketing;
- Right to object to processing for scientific, historical or statistical purposes;
- Right to not be evaluated on the basis of automated processing;
- Right to withdraw consent at any time;
- Right to be notified about a data breach;
- Right to an effective judicial remedy against a supervisory authority;
- Right to lodge a complaint with supervisory authority;
- Right to an effective judicial remedy against a controller or processor;
- Right to compensation.

The Organisation shall maintain procedures, policies and notices to ensure that data subjects are informed about their rights.

Lawful processing

We will only process personal data where a lawful basis for processing exists. Specifically, where:

- the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a **legal obligation** to which the controller is subject;

- processing is necessary in order to protect the **vital interests** of the data subject or of another natural person;
- processing is necessary for the **performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller.

Special categories of personal data will not be processed unless a specific lawful basis listed in Article 9 of the GDPR applies.

Information Commissioner's Office

For the purposes of data protection, The Organisation is a data controller; responsible for the determination of the purposes and means of the processing of personal data and where the purposes and means of such processing takes place. As such, The Organisation is supervised by the Information Commissioner's Officer and will pay the data protection fee required by law.

The Data Protection Officer will be the principal point of contact with the Information Commissioner's Office.

Data Sharing

Data will be shared with third parties only where a lawful basis exists.

Where data is shared with third-party processors, they will only process data with the explicit instructions (either contractual or through a data sharing agreement) of The Organisation and shall not hold or process the data for any other purpose. The minimum data required for the processing task will be provided for the processing. Any third-party processors, where contracts or data sharing agreements are required for the processing to take place will be required to provide evidence of their commitment to GDPR compliance.

Where we have a legal obligation to share information with law enforcement, agencies and government bodies for legitimate purposes relating to criminal justice and taxation we will do so.

We will share information if there is an issue that jeopardises the safety or security of staff, students of school visitors.

Data may be shared for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In this case, efforts will be made to ensure the minimum data required is shared and if possible, anonymised prior to sharing.

Data Breaches

In the case of a personal data breach, The Organisation 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 Information Commissioner's Office, 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 Information Commissioner's Office is not made within 72 hours, it shall be accompanied by reasons for the delay.

In order to evaluate the personal data breach The Organisation shall inform and involve the Data Protection Officer in the assessment of the breach and in the execution of the data breach procedure to contain and manage the breach.

The notification shall at least:

- 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;
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;
- 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;
- 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.

The Organisation shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken in a data breach log. The log shall enable the Information Commissioner's Officer to verify compliance with the data breach rules and raise awareness of minor breaches that may assist in the identification of new data handling processes and training requirements.

Examples of data breaches

- Loss or theft of paper records or loss or theft of equipment on which data is stored e.g. a laptop, mobile phone, tablet device or memory stick;
- A letter or email containing personal and/or confidential data sent to the wrong address (including internal staff or third parties) or an email to an unauthorised group of email boxes;
- Personal data disclosed orally in error in a meeting or over the phone – including "blogging" where information is obtained by deceiving The Organisation, or where information has been disclosed without confirming the true identity of the requester;
- Unauthorised access to information classified as personal or confidential e.g. attaching documents to an outlook diary appointment that is openly accessible;

- Posting information on the world wide web or on a computer otherwise accessible from the Internet without proper information security precautions;
- Sensitive information left on a photo-copier or on a desk in County Council premises;
- Unauthorised alteration or deletion of information;
- Not storing personal and confidential information securely;
- Not ensuring the proper transfer or destruction of files after closure of offices/buildings e.g. not following building decommissioning procedures;
- Failure to safeguard/remove personal data on office equipment (including computers and smart phones) before disposal/sale.

Breaches caused by IT Security Incidents

Examples:

- Unauthorised access to IT systems because of misconfigured and/or inappropriate access controls;
- Hacking or phishing attacks and related suspicious activity;
- Virus or malware attacks and related suspicious activity;
- ICT infrastructure-generated suspicious activity;
- Divulging a password to another user without authority.

Subject Access Requests

The Organisation is committed to:

- Ensuring that individuals' rights to their own personal information can be appropriately exercised;
- Providing adequate training for staff to recognise and handle subject access requests;
- Ensuring that everyone handling personal information knows where to find further guidance on individuals' rights in relation to their own personal information;
- Ensuring that queries about individuals' rights to their own personal information are dealt with effectively and promptly;
- Being fair and transparent in dealing with a subject access request;
- Logging all subject access requests to assist the Information Commissioner's Office with any complaints related to subject access as well as identifying any issues that may assist in the identification of new data handling processes and training requirements.

All staff are responsible for ensuring that any request for information they receive is dealt with in line with the requirements of the GDPR and in compliance with this policy.

All staff have a responsibility to recognise a request for information and ensure it is passed to the responsible member of staff and/or the Data Protection Officer within two working days.

Dealing with a subject access request (SAR)

What must I do?	Why?	How?
Be clear about the nature of the request and identify what information is being requested.	Being clear about the nature of the request will enable you to decide whether the request needs to be dealt with in accordance with statutory requirements, who needs to deal with the request, and/or whether this is business as usual (BAU). If needed ask the submitter of the request for clarity.	Review the request and identify: If the request is for the personal information of the requester or made by an individual on behalf of another person (e.g. on behalf of a child or an adult lacking capacity) – this is a subject access request; If the request is for non-personal information – this may be dealt with as BAU or formally under the Freedom of Information Act 2000 (the FOIA) or the Environmental Information Regulations 2004 (the EIR). NB: The request can be received in a range of different formats e.g. letter, email, a completed form, or can be made via social media (e.g. a Facebook page or Twitter account).
If the request is a SAR the request must be forwarded to the responsible member of staff (usually the Headteacher) and the Data Protection Officer within two working days of receipt of the request.	The GDPR stipulates that SARs must be completed within one month of the request – but in reality as soon as possible.	Log the SAR in the subject access request log and inform all appropriate staff required to deal with the request.
If the information requested is for non-personal information i.e. is organisational or statistical information, this will fall under the FOIA or EIR, or BAU and will be dealt with, as follows:- All non-routine FOIA or EIR requests must be forwarded to the responsible member of staff (usually the Headteacher) and the	The FOIA and EIR stipulates that requests must be completed within 20 working days of the request – therefore the more swiftly request are being dealt with, the more likely The Organisation will meet its statutory deadlines. BAU requests need to be dealt with by an individual in that	If the request is for non-routine/FOIA/EIR information contact the responsible member of staff (usually the Headteacher) and the Data Protection Officer.

What must I do?	Why?	How?
Data Protection Officer within two working days of receipt of the request.	particular service area who can identify and locate the information requested and provide a response within a reasonable timeframe.	
If the information requested is for the personal information of an individual for use in a criminal investigation by the police, or any other agency investigating criminal offences, this will fall under either the regulatory Investigative Powers Act 2000 (RIPA) or Data Protection Act 2018. The request can be for either hard copy or any type of electronic information including email traffic ie the time and information that an email is sent. The request must be forwarded to the responsible member of staff (usually the Headteacher) and the Data Protection Officer within two days.	It is in the public interest that requests are identified and dealt with as quickly as possible.	Scan and email the request to the responsible member of staff (usually the Headteacher) and the Data Protection Officer as needed.

Data Protection Officer

The named Data Protection Officer for The Organisation is: **Stuart Lee**

The Data Protection Officer can be contacted at: dpo@dataprotection.education

The Organisation shall maintain a named Data Protection Officer to represent the rights of data subjects.

The Organisation shall ensure that the data protection officer is involved properly and in a timely manner, in all issues which relate to the protection of personal data.

The Organisation shall support the data protection officer in performing the responsibilities outlined below by providing resources necessary to carry out those tasks and access to personal data and processing operations. The Data Protection Officer shall maintain his or her expert knowledge.

The Organisation shall ensure that the data protection officer does not receive any instructions regarding the exercise of their tasks. They shall not be dismissed or penalised by the controller or the processor for performing his tasks.

The data protection officer shall directly report to the highest management level of The Organisation, as needed and report to the Board of Governors at least once a year.

Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks.

The Data Protection Officer shall have the following responsibilities:

- Review of all data processing activities (inventory / mapping);
- Conduct of regular health checks/audits and issue recommendations;
- Assistance with data protection impact assessments and monitoring performance;
- Monitoring and advice relating to subject access requests and data breaches;
- Assisting schools with maintenance of records;
- Monitoring and advice relating to FOI and other information requests;
- Co-operation with, and act as the contact point for the supervisory authority, the Information Commissioner's Office;
- Act as the contact point for data subjects to deal with requests and complaints;
- Training staff.

Data Security

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, The Organisation will implement appropriate technical and organisational measures to ensure a level of security of the processing of Personal Data appropriate to the risk.

These measures shall include as appropriate:

- measures to ensure that the Personal Data can be accessed only by authorised personnel for the purposes agreed in the record of processing activity and outlined in the privacy notice;
- in assessing the appropriate level of security account shall be taken in particular of all the risks that are presented by processing, for example from accidental or unlawful destruction, loss, or alteration, unauthorized or unlawful storage, processing, access or disclosure of personal data;

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regular testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing of personal data;
- measures to identify vulnerabilities with regards to the processing of personal data in systems used to provide services to The Organisation.

Photography and Videos

Photographs and videos will only be collected and stored with a documented lawful basis.

Photographs and videos will be used where they are deemed essential for performing the public task of the school or relative to providing education. Where photographs are required for other purposes, these purposes will be documented and explicit consent will be sought.

The retention period for photographs and videos will be documented in the retention policy. At the end of the retention period photographs will either be destroyed or they may be retained as photos for archiving purposes in the public interest.

CCTV

We do not currently have CCTV installed in school

Retention Policy

The Organisation will not keep personal data longer than necessary and will maintain a retention schedule outlining the retention requirements of electronic and paper records. The Organisation will retain the minimum amount of information that it requires to carry out its' statutory functions and the provision of services.

In circumstances where a retention period of a specific document has expired, checks will be made to confirm disposal and consideration given to the method of disposal to be used based on the data to be disposed of. These checks will include:

- Have the documents been checked to ensure they are appropriate for destruction?

- Is retention required to fulfil statutory obligations or other regulatory obligations, including child protection?
- Is retention required for evidence?
- Is retention required to meet the operational needs of the service?
- Is retention required because the document or record is of historic interest, intrinsic value or required for organisational memory?

Training

The Organisation shall ensure that all members of staff receive data protection training, including information handling appropriate to ensure data protection competence in their role, a minimum of every two years.