Norwood Green Junior School

GDPR Data Protection Policy

Policy ratified by the GB: June 2026

Policy to be reviewed: June 2027

Contents

1. Introduction **4**

2. Scope **4**

3. Roles and responsibilities **5**

Governing Body *5*

Data Protection Officer (DPO) *5*

Headteacher *5*

All Staff *5*

4. Definitions **5**

5. Policy **7**

Governance *7*
Policy Dissemination and Enforcement 7
Data Protection by Design 8
Compliance Monitoring 8

Principles *8*
Data Protection 8
Accountability 9

Data Collection *9*
Data Subject Consent 9
External Privacy Notes 10

Data Use *10*
Data Processing 10
Sensitive Personal Data 10
Data Quality 11
Direct Marketing 12
Photos and Videos 12
CCTV 13

Artificial Intelligence *13*

Data Retention *13*

Data Protection *13*

Data Subject Rights *14*

Parental requests to see the educational record *15*

Responding to subject access requests *15*

Third-Party Data *16*

Law Enforcement Requests and Disclosures *16*

Data Protection Training *16*

Data Transfer *17*
Transfers to Third Parties 17

Complaints Handling *17*

Breach Reporting *18*

6. Policy Maintenance and Publication 18

7. Related Documents 18

8. Appendix A 19

Incident Management 19
Objective 19
Purpose 20
General Definitions 20
Scope 21
Security of information 21
Procedure for incident handling 22

9. Appendix B 24

Breach Management Plan 24
Containment and recovery 24
Assessment of ongoing risks 24
Breach notification 25
Evaluation and response 26
Incident severity assessment 26
Categorising Personal Data Breaches 27
Notification of data breaches to the ICO 28
Incident management 29
Personal data breach register 29
Incident management flow diagram 30
ICO Incident Report Form 31
Internal Incident Report Form 32
Special Categories of Data Overview 33

10. Appendix C 34

Individual Rights 34
The right to be informed 34
The right of access 35
Unfounded or excessive requests 35
Concerns about "serious harm" 36
Information that includes others' personal data 36
Other exemptions 36
The right to rectification 37
The right to erasure/be forgotten 38
The right to restrict processing 38
The right to data portability 39
The right to object 40
Rights relating to automated decision making and profiling 41

1. Introduction

Norwood Green Junior School is committed to conducting its business in accordance with all applicable Data Protection laws and regulations. This policy meets the requirements of the UK General Data Protection Regulations (UK GDPR) – the EU GDPR was incorporated into UK legislation with some amendments by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulation 2020 and the Data Protection Act 2018 (DPA 2018). It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department of Education (DfE) on Generative artificial intelligence in education. It also reflects the ICO's guidance for the use of surveillance cameras and personal information. In addition, this policy complies with our funding agreement and articles of association.

This policy details expected behaviours of Norwood Green Junior School's employees and third parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to a pupil, parent or staff member of Norwood Green Junior School and irrespective of the media used to store the information.

Personal Data is any information which relates to an identified or Identifiable Natural Person. Personal Data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process Personal Data.

An organisation that handles personal data and makes decisions about its use is known as a Data Controller. Norwood Green Junior School, as a Data Controller, processes personal data relating to parents, pupils, staff, governors, visitors and others. The school is registered with the ICO and has paid its data protection fee to the ICO as legally required. The school is responsible for ensuring compliance with the Data Protection requirements outlined in this policy.

The Trustees of Norwood Green Junior School are fully committed to ensuring continued and effective implementation of this policy and expects all Norwood Green Junior School employees and third parties to share in this commitment.

Any breach of this policy will be taken seriously and may result in disciplinary action.

2. Scope

- This policy applies to all staff employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action. This policy also applies to all activities undertaken by Norwood Green Junior School where a Data Subject's personal data is processed in the context of the general educational activities of the school.
- This policy applies to all processing of personal data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.
- This policy has been designed to establish a baseline standard for the processing and protection of personal data by all Norwood Green Junior School employees. Where national law imposes a requirement that is stricter than that imposed by this policy, the requirements in national law must be followed. Furthermore, where national law imposes a requirement that is not addressed in this policy, the relevant national law must be adhered to.
- The protection of personal data belonging to Norwood Green Junior School employees is not within the scope of this policy.

3. Roles and responsibilities

Governing Body

The Governing body has overall responsibility for ensuring that the school complies with all relevant data protection obligations

Data Protection Officer (DPO)

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. The DPO is also the first point of contact for individuals whose data the school processes. The DPO for our school is Miss Blakeburn who can be contacted by emailing dpo@ngjs.hounslow.sch.uk.

Headteacher

The Headteacher acts as the representative of the data controller on a day-to-day basis.

All Staff

Staff are responsible for

- collecting, storing and processing any personal data in accordance with this policy.
- informing the school of any changes to their personal data such as a change of address.
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way.
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK.
    - If there has been a Data breach
    - Whenever they are engaging in a new, or change in, activity that may affect the privacy rights of individuals.
    - if they need help with any contracts or sharing Personal Data with third parties.

4. Definitions

TERM	DEFINITION
ANONYMISATION	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person.
BINDING CORPORATE RULES	The Personal Data protection policies used for the transfer of Personal Data to one or more Third Countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

CONSENT	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.
CUSTOMER	Any past, current or prospective Norwood Green Junior School customer.
DATA CONTROLLER	A natural or legal person, Public Authority, Agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
DATA PROCESSOR	A natural or legal person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data Controller.
DATA PROTECTION	The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction.
DATA PROTECTION OFFICER (DPO)	The person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the Company data privacy team with responsibility for data protection compliance.
DATA SUBJECT	Anyone 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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
EEA	The 28 countries in the EU, and Iceland, Liechtenstein and Norway.
EMPLOYEE	An individual who works part-time or full-time for Norwood Green Junior School under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties – includes temporary employees and independent contractors.

ENCRYPTION	The process of encoding a message or information in such a way that only authorised parties can access it.
INFORMATION COMMISSIONER'S OFFICE (ICO)	An independent Public Authority in the UK responsible for monitoring the applicatic of the relevant Data Protection regulation set forth in national law.
PERSONAL DATA BREACH	A breach of security leading to the accidental or unlawful destruction, loss, alteratic unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.
PROCESS, PROCESSED, PROCESSING	Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means. Operations performed may include 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.
PROFILING	Any form of automated processing of Personal Data, where Personal Data is used to evaluate specific or general characteristics relating to a data subject. In particular to analyse or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement.
PSEUDONYMISATION	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) without a 'key' that allows the data to be re-identified.
SPECIAL CATEGORIES OF DATA	Personal Data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.

5. Policy

Governance

Policy Dissemination and Enforcement

The Trustees of Norwood Green Junior School have overall responsibility in ensuring that the school complies with all relevant data protection obligations and that all its employees responsible for the processing of personal data are aware of, and comply with, the contents of this policy. In addition, Norwood Green Junior School will make sure all third parties engaged to process personal data on their behalf (i.e. their Data Processors) are aware of, and comply with, the contents of this policy. Assurance of such compliance must be obtained from third parties, whether companies or individuals, prior to granting them access to personal data controlled by Norwood Green Junior School.

Data Protection by Design

Norwood Green Junior School will complete data protection impact assessments where the school's processing of personal data presents a high risk to the rights and freedoms of individuals, and when introducing new technologies/systems where the system or process stores personal data (the DPO will advise on this process).

Compliance Monitoring

To confirm that an adequate level of compliance is being achieved by Norwood Green Junior School in relation to this policy, Norwood Green Junior School will carry out an annual Data Protection compliance audit. Each audit will assess compliance with this policy and operational practices in relation to the protection of Personal Data, including:

- the assignment of responsibilities
- raising awareness
- training of Employees
- adequacy of organisational and technical controls to protect Personal Data
- records management procedures (including data minimisation)
- adherence to the qualified rights of the Data Subject
- Privacy by Design and Default
- consent for direct marketing
- Personal Data transfers
- Personal Data incident management (including Personal Data breaches)
- Personal Data complaints handling
- 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.

Any major deficiencies identified will be reported to and monitored by the Trustees of the school.

Principles

Data Protection

The UK GDPR is based on data protection principles. Norwood Green Junior School must comply with these principles to govern its collection, use, retention, transfer, disclosure and destruction of Personal Data. The principles say that personal data must be:

PRINCIPLE	DEFINITION
Processed lawfully, fairly and in a transparent manner	This means Norwood Green Junior School must tell the Data Subject what processing will occur (transparency), the processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).
Collected for specified, explicit and legitimate purposes	This means Norwood Green Junior School must specify exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.
Adequate, relevant and limited to what is necessary relation to fulfil the purposes for which they are processed	This means Norwood Green Junior School must not store any personal data beyond what is strictly required.

Accurate and, where necessary, kept up to date	This means Norwood Green Junior School must have in place processes for identifying and addressing out-of-date, incorrect and redundant personal data.
Kept for no longer than is necessary for the purposes for which it is processed	This means Norwood Green Junior School must, wherever possible, store personal data in a way that limits or prevents identification of the Data Subject. Personal data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary.
Processed in a way that ensures it is appropriately secure	Norwood Green Junior School must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data are maintained at all times including protection against unauthorised or unlawful processing, and against accidental loss, destruction damage.

Accountability

The Data Controller shall be responsible for, and be able to demonstrate, compliance. This means Norwood Green Junior School must demonstrate that the six Data Protection Principles (outlined above) are met for all Personal Data for which it is responsible.

Data Collection

Personal Data should be collected only from the Data Subject/parent/carer of the Data Subject unless one of the following applies:

- The nature of the business purpose necessitates collection of the Personal Data from other persons or bodies.
- The collection must be carried out under emergency circumstances 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:
    - the Data Subject has received the required information by other means
    - the information must remain confidential due to a professional secrecy obligation
    - a national law expressly provides for the collection, Processing or transfer of the Personal Data.

Where it has been determined that notification to a Data Subject is required, notification should occur promptly, but in no case later than:

- one calendar month from the first collection or recording of the Personal Data
- at the time of first communication, if used for communication with the Data Subject
- at the time of disclosure, if disclosed to another recipient.

Data Subject Consent

Norwood Green Junior School will obtain Personal Data only by lawful and fair means and, where appropriate, with the knowledge and consent of the individual concerned.

Norwood Green Junior School shall establish a system for obtaining and documenting Data Subject consent for the collection, processing, and/or transfer of their personal data. The system must include provisions for:

- ensuring the request for consent is presented in a manner which is clearly distinguishable from any other matters
- ensuring the request for consent is made in an intelligible and easily accessible form, and uses clear and plain language
- ensuring the consent is freely given
- documenting the date, method and content of the disclosures made, as well as the validity, scope, and volition of the Consents given

- providing a simple method for a Data Subject to withdraw their consent at any time.

External Privacy Notes

The school website will include an online 'Privacy Notice' and an online 'Cookie Notice' fulfilling the requirements of applicable law.

Data Use

Data Processing

Norwood Green Junior School will process personal data in accordance with data protection regulations and applicable contractual obligations. The school will not process personal data unless at least one of the following requirements are met:

- The Data Subject has given consent to the processing of their personal data for a specific purpose.
- Processing of the personal data 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 Data 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 Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject, in particular where the Data Subject is a child).

Sensitive Personal Data

Sensitive personal data include the following:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- data concerning sex life, sexual orientation or health
- genetic data
- biometric data, where processed in a manner that will uniquely identify a person.

Norwood Green Junior School will only process sensitive personal data where the Data Subject expressly consents to such processing or where one of the following conditions apply:

- the processing is necessary for the school to discharge its legal duty
- the processing is specifically authorised or required by law
- the processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent.

Where sensitive personal data is being processed, Norwood Green Junior School will adopt additional protection measures.

For special categories of personal data, we will also meet 1 of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**

- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**

- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent

- The data has already been made **manifestly public** by the individual

- The data needs to be processed for the establishment, exercise or defence of **legal claims**

- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law

- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law

- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

- For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**

- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent

- The data has already been made **manifestly public** by the individual

- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**

- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

Data Quality

Norwood Green Junior School will adopt all necessary measures to ensure that the personal data it collects and processes is complete and accurate in the first instance, and is updated to reflect the current situation of the Data Subject.

The measures adopted by Norwood Green Junior School to ensure data quality include:

- correcting personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification

- keeping personal data only for the period necessary, to satisfy the permitted uses or applicable statutory retention period
- the removal of personal data if in violation of any of the Data Protection principles or if the personal data is no longer required
- restriction, rather than deletion of personal data, insofar as:
    - a law prohibits erasure
    - erasure would impair legitimate interests 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.

Direct Marketing

As a general rule, Norwood Green Junior School will not send promotional or direct marketing material to parents, pupils, staff or stakeholders through digital channels such as mobile phones, email and the Internet, without first obtaining their consent.

The GDPR and Privacy and Electronic Communications (which governs Direct Marketing Activities within the EU) directs the GDPR standard for consent. That is:

- The consent must be freely given, specific, informed and unambiguous.
- The consent must be expressed by a statement or clear affirmative action. Silence, pre-ticked boxes or inactivity should therefore not constitute consent.
- The consent must be as easy to withdraw as it was to provide consent in the first place.
- The organisation must be able to demonstrate that the individual has consented.
- The consent language must be intelligible and use clear and plain language.

Contacting recipients via email to establish whether consent is in place also constitutes direct marketing and is prohibited without first obtaining consent from the Customer. The request for consent must be clearly distinguished from other matters. Prior consent, before sending electronic communications for direct marketing purposes will be required. This would mean if Norwood Green Junior School were proposing to email parents or prospective donors of financial or material donations the Norwood Green Junior School would have to obtain prior consent.

Photos and Videos

As part of our school activities, Norwood Green Junior School may take photographs and record images of individuals within the school. The school will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. The school will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, the school will delete the photograph or video and not distribute it further. When using photographs and videos in this way the school will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Where personal data of pupils, including photographs, is used for digital marketing purposes such as an online prospectus and school website, the parent/carer must be informed at the point of initial contact that they have the right to object, at any stage, to having their data processed for such purposes. Where an

objection is made all marketing-related processing of the personal data will stop and details will be kept on a list with a record of the decision.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

See our **Camera and Image Use Policy** for more information on our use of photographs and videos.

CCTV

Norwood Green Junior School uses CCTV in various locations around the school site to ensure it remains safe, secure and for safeguarding purposes. We will follow the ICO's guidance for the use of CCTV and comply with data protection principles.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed the Headteacher.

Artificial Intelligence

Artifical Intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as Chat GPT and Google Bard. Norwood Green Junior School recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data. To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Norwood Green Junior School will treat this as a data breach, and will follow the personal data breach procedure.

Data Retention

To ensure fair processing, personal data will not be retained by Norwood Green Junior School for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed.

The length of time for which Norwood Green Junior School needs to retain personal data is set out in the **Information Management Data Retention Policy**. This takes into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods. All personal data should be securely deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it. For example, we will shred paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Data Protection

Norwood Green Junior School will adopt physical, technical, and organisational measures to ensure the security and protect the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.
- Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

- Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes

This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

A summary of the personal data related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which personal data is processed by use of passwords that are changed on a regular basis.
- Prevent persons entitled to use a data processing system from accessing personal data beyond their needs and authorisations.
- Ensure that personal data in the course of electronic transmission during transport cannot be read or copied by the use of encryption.
- Ensure encryption software is used to protect all portable devices and removable media, such as laptops and USB devices when processing personal data away from Norwood Green Junior School
- Ensure that access logs are in place to establish whether, and by whom, the personal data was entered into, modified or removed from a data processing system.
- Ensure that in the case where processing is carried out by a Data Processor, the data can be processed only in accordance with the instructions of the Data Controller.
- Ensure that personal data is protected against undesired destruction or loss.
- Ensure that personal data is not kept longer than necessary.
- Ensure that paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use.
- Ensure that papers containing personal data are not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Regularly evaluate and test the effectiveness of safeguards to ensure security of processing of personal data.

Data Subject Rights

The process for attending to the following Data Subject rights is outlined in **Appendix C** - **Individual Rights**:

- information access
- objection to Processing.
- objection to automated decision-making and Profiling
- restriction of Processing
- data portability
- data rectification
- data erasure.

No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the collection, processing, use and storage of their personal data
- The source(s) of the personal data, if it was not obtained from the individual
- The categories of personal data concerned
- Who the data has been, or will be, shared with and the location of those recipients

- How long the data will be stored for, or if that isn't possible, the criteria used to determine the period
- the retention periods applied to the data
- a summary of the security measures in place to protect the data
- request to erase personal data, if it is no longer necessary in relation to the purposes for which it was collected or processed, or to rectify inaccurate data or to complete incomplete data.
- The right to lodge a complaint with the IOC or other supervisory authority

Parental requests to see the educational record

As an Academy there is no automatic parental right of access to a child's educational record. Parents are entitled to an annual report relating to the child under the Education (Independent Schools Standard) Regulation 2014. However the personal data held by the school belongs to the child and where a child does not have the ability to request the data the parent or those with parental responsibility can request the data on their behalf. The request should be put to the school in writing as a subject access request. The school will check to ensure there are no restrictions in place relating to sharing information with the parent concerned for example in cases of separated parents or looked after children.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts
- If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

- When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

The timescale for responding to a SAR does not begin until the school has received the requested information. However, you should request ID documents promptly. Data Subjects shall have the right to require Norwood Green Junior School to correct or supplement erroneous, misleading, outdated, or incomplete personal data.

Please refer to the **Individuals Rights – Appendix C** for guidance and procedures for responding to such requests.

Third-Party Data

It should be noted that situations may arise where providing the information requested by a Data Subject would disclose personal data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

When personal data is collected indirectly (for example, from a third party or publicly available source), Norwood Green Junior School will provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. Norwood Green Junior School will also check that the personal data was collected by the third party in accordance with the GDPR and on a basis which contemplates proposed processing of that personal data.

Law Enforcement Requests and Disclosures

In certain circumstances, it is permitted that Personal Data be shared without the knowledge or consent of a Data Subject. This is the case where the disclosure of the personal data is necessary for any of the following purposes:

- the prevention or detection of crime;
- the apprehension or prosecution of offenders
- the assessment or collection of a tax or duty
- by order of a court or by any rule of law.

Data Protection Training

All Norwood Green Junior School employees and employees that have access to personal data will have their responsibilities outlined to them as part of their staff induction training. In addition, Norwood Green Junior School and will provide regular Data Protection training and procedural guidance for staff.

The training and procedural guidance set forth will consist of, at a minimum, the following elements:

- the Data Protection Principles set out on page 7
- each Employee's duty to use and permit the use of personal data only by authorised persons and for authorised purposes
- the need for, and proper use of, the forms and procedures adopted to implement this policy
- the correct use of passwords, security and other access mechanisms
- the importance of limiting access to personal data, such as by using password protected screen savers and logging out when systems are not being attended by an authorised person
- securely storing manual files, printouts and electronic storage media
- information on how to detect a phishing email
- proper disposal of personal data by using secure shredding facilities
- any special risks associated when conducting educational activities or duties.

Data Transfer

Norwood Green Junior School may transfer personal data to internal or Third-Party recipients located in another country where that 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 countries lacking an adequate level of legal protection (i.e. Third Countries), they must be made in compliance with an approved transfer mechanism.

Norwood Green Junior School may only transfer personal data where one of the transfer scenarios listed below applies:

- the Data Subject has given Consent to the proposed transfer.
- the transfer is necessary for the performance of a contract with the Data Subject
- the transfer is necessary for the implementation of pre-contractual measures taken in response to the Data Subject's request
- the transfer is necessary for the conclusion or performance of a contract concluded with a Third Party in the interest of the Data Subject.
- the transfer is legally required on important public interest grounds
- the transfer is necessary for the establishment, exercise or defence of legal claims
- the transfer is necessary in order to protect the vital interests of the Data Subject.

Transfers to Third Parties

Norwood Green Junior School will only transfer personal data to, or allow access by, Third Parties when it is assured that the information will be processed legitimately and protected appropriately by the recipient. Where Third-Party processing takes place, Norwood Green Junior School will first identify if, under applicable law, the Third Party is considered a Data Controller or a Data Processor of the Personal Data being transferred.

Where the Third Party is deemed to be a Data Controller, Norwood Green Junior School will enter into an appropriate agreement with the Controller to clarify each party's responsibilities in respect to the personal data transferred.

Where the Third Party is deemed to be a Data Processor, Norwood Green Junior School will enter into an adequate processing agreement with the Data Processor. The agreement must require the Data Processor to protect the personal data from further disclosure and to only process personal data in compliance with Norwood Green Junior School instructions. In addition, the agreement will require the Data Processor to implement appropriate technical and organisational measures to protect the personal data, as well as procedures for providing notification of Personal Data Breaches.

When outsourcing services to a Third Party (including Cloud Computing services), Norwood Green Junior School will identify whether the Third Party will process personal data on its behalf and whether the outsourcing will entail any Third Country transfers of Personal Data.

Regular audits of processing of personal data performed by Third Parties, especially in respect of technical and organisational measures they have in place, should be undertaken. Any major deficiencies identified will be reported to and monitored by the Trustees of Norwood Green Junior School.

Complaints Handling

Data Subjects with a complaint about the processing of their personal data should put forward the matter in writing. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. Norwood Green Junior School will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation with the Data Subject, then the Data Subject should be advised that they may, at their option, contact the Information Commissioner's Office (ICO).

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 Officer providing a description of what occurred. Notification of the incident can be made via e-mail to dpo@ngjs.hounslow.sch.uk or by calling 0208 574 1726. The Data Protection Officer should update the internal breach log, including pertinent facts relating to the incident, effects and remedial actions taken.

All reported incidents will be investigated to confirm whether or not a Personal Data Breach has occurred. When appropriate, Norwood Green Junior School will inform the ICO within 72 hours of becoming aware of the breach. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website, which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

Where there is a risk of damage to the Data Subject, the affected Data Subjects should be advised of the personal data breach.

Guidance can be found in the **Incident Management information – Appendix A**.

6. Policy Maintenance and Publication

- This policy shall be available to all Employees through the Norwood Green Junior School staff shared area. A hard copy will also be available in the staffroom.
- This policy will be reviewed annually and shared with the full governing body.

Note: the annual review frequency here reflects the Department for Education's recommendation in its advice on statutory policies. This document has now been withdrawn, however the DfE's latest guidance does not include data protection in its list of statutory policies for maintained schools or academies, including free schools, however it is a legal requirement that the school has data protection policies and procedures in place.

7. Related Documents

This data protection policy is linked to our:

- Freedom of information Policy and Publication Scheme
- Information Management and Data Retention Policy
- Camera & Image Use Policy

8. Appendix A

Incident Management

Norwood Green Junior School is responsible for protecting the information it holds and is legally required under the General Data Protection Regulation (GDPR) to ensure the security and confidentiality of personal information processed.

Every care is taken to protect information and to avoid a security incident, especially where the result is a data breach when personal information is lost or disclosed inappropriately to an unauthorised person. In the unlikely event of such a security incident, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. We will investigate all security incidents classified as serious using a set plan and follow a Breach Management Plan in the event of a data breach.

This Incident Management protocol (GDPR Data Breach) is in line with the current Commissioner's Office (ICO) guidance for reporting, managing and investigating breaches of personal data.

Norwood Green Junior School takes information security very seriously and understands the necessity to take prompt action in the event of any actual or suspected breaches of information security or confidentiality to avoid the risk of harm to individuals, damage to operational business and severe financial, legal and reputational costs to the school.

The GDPR introduces a mandatory requirement to report certain types of personal data breaches, which are likely to result in a risk to the rights and freedoms of individuals, to the Information Commissioner's Officer (ICO). The implementation of this Policy will ensure that personal data breaches are thoroughly investigated, with adequate remedial actions put in place and breach notification requirements complied with. In each case, specific GDPR provisions will be followed in a timely manner and within the specified timeframes.

GDPR Article 33(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 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.'

Norwood Green Junior School understands the severity of a failure to notify a reportable incident to the ICO. Failure to notify may lead to an administrative fine up to €20,000,000 or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Objective

The objective is to support the prompt and consistent management of information security incidents to minimise any harm to individuals such as pupils, parents and staff or the school.

This supports the strategic business aims and objectives of Norwood Green Junior School by:

- ensuring that Norwood Green Junior School has implemented an effective information incident management and response mechanism that supports the implementation and sharing of lessons learned
- ensuring that there is a considered and agreed incident response and communications plan available, including the reporting of 'perceived' or 'actual' breaches
- ensuring that the investigation and reporting of data protection incidents conform to GDPR requirements and do not conflict with the school's policies and procedures
- facilitating the analysis of incident records to determine common risk patterns to raise awareness and implement preventative measures

- ensuring that every member of staff at Norwood Green Junior School understands the importance of reporting and managing information security incidents to reduce the risk of a future breach and to mitigate the impact of any potential breach.

Purpose

The purpose is to provide a framework for reporting and managing:

- security incidents affecting Norwood Green Junior School's information and IT systems
- losses of information
- near misses and information security concerns.

Everyone has an important part to play in reporting and managing information security incidents in order to mitigate the consequences and reduce the risk of future breaches of security.

General Definitions

TERM	DEFINITION
DATA CONTROLLER	A natural or legal person, Public Authority, Agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
DATA PROCESSORS	A natural or legal person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data Controller.
DATA PROTECTION	The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction.
DATA SUBJECT	Anyone 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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
ENCRYPTION	The process of encoding a message or information in such a way that only authorised parties can access it.
INFORMATION COMMISSIONER'S OFFICE (ICO)	An independent Public Authority in the UK responsible for monitoring the application of the relevant Data Protection regulation set forth in national law.

PERSONAL DATA BREACH	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.
PROCESS, PROCESSED, PROCESSING	Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means. Operations performed may include 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.

Scope

An information security incident is any event that has the potential to affect the confidentiality, integrity or availability of information in any format. Examples of a Personal Data Breach include the following (please note, this is not an exhaustive list):

- the loss or theft of data or information
- unlawful disclosure or misuse of confidential data/the disclosure of confidential information to unauthorised individuals
- using personal data in a way incompatible with the originally specified purpose
- information security breaches and inappropriate invasion of people's privacy
- personal data breaches which could lead to identity fraud or have other significant impact on individuals
- inappropriate access controls leading to unauthorised use
- any incident which involves actual or potential failure to meet the requirements of the GDPR and/or the common law of confidentiality
- loss or theft of paper records, data or equipment such as tablets, laptops and smartphones on which data is stored
- inappropriate access controls allowing unauthorised use of information
- attempts to gain unauthorised access to computer systems e.g. hacking
- virus or other security attacks on IT equipment systems or networks
- 'blagging offence, where information is obtained by deception
- breaches of physical security e.g. forcing of doors or windows into secure room, or filing cabinet containing confidential information left unlocked in accessible area
- leaving IT equipment unattended when logged in to a user account without locking the screen to stop others accessing information.

This applies to all users of Norwood Green Junior School information. Users include all employees (including temporary workers), suppliers and visitors who may have access to Norwood Green Junior School information. All users **must** understand and adopt this protocol and are responsible for ensuring the safety and security of Norwood Green Junior School systems and the information that they use or manipulate. This includes both data stored electronically and in any other form.

Security of information

The new GDPR principle of accountability requires the Data Controller to be responsible for and to be able to 'demonstrate' and 'evidence' compliance with the Data Protection Principles.

Norwood Green Junior School is committed to putting in place adequate technical and organisational safeguards to prevent information security incidents and to establish immediately whether a breach has taken place. Technical safeguards can be thought of as physical protection ranging from ICT passwords and

firewalls to building security, while organisational safeguards are aimed at employees (e.g. ensuring adequate training, policies and procedures are in place).

An Incident can be caused by a number of factors, such as:

- negligence or human error
- unauthorised or inappropriate access, including processing confidential personal data without a legal basis
- loss or theft of information or equipment on which information is stored
- systems or equipment failure
- accidents
- unforeseen circumstances such as fire, flood and other environmental factors
- inappropriate access, viewing information for purposes other than specified/authorised, e.g. an individual browsing a record about an ex-partner to find their current address
- unauthorised access, using other people's user IDs and passwords
- poor physical security
- inappropriate access controls allowing unauthorised use
- lack of training and awareness
- hacking attacks
- 'blagging' offences, where information is obtained by deception.

Procedure for incident handling

Events and weaknesses need to be reported at the earliest possible stage as they need to be assessed by the Headteacher.

Suspected Cyber Attack

a. Security events, for example a virus infection found within a malicious email attachment, could quickly spread and cause data loss across the organisation. All users must understand, and be able to identify, that any unexpected or unusual behaviour on the workstation could potentially be a software malfunction. If an event is detected users must:

    - note the symptoms and any error messages on screen
    - disconnect the workstation from the network if an infection is suspected (with assistance from the relevant staff member responsible for ICT in the school)
    - not use any removable media (for example USB memory sticks) that may also have been infected.

b. All suspected security events should be reported immediately to the IT Managed Service (Gaia) and the Headteacher.

c. The IT Managed Service (Gaia) will require you to supply further information, the nature of which will depend upon the nature of the incident. However, the following information must be supplied:

    - contact name and contact number of person reporting the incident
    - the type of data, information or equipment involved
    - whether the loss of the data puts any person or other data at risk
    - location of the incident
    - date and time the security incident occurred
    - location of data or equipment affected
    - type and circumstances of the incident.

Other Incidents

If the Information Security event is in relation to paper or hard copy information, for example personal information files that may have been stolen from a filing cabinet, this must be reported to the Headteacher

Collection of Evidence

If an incident may require information to be collected for an investigation, strict rules must be adhered to. The collection of evidence for a potential investigation must be approached with care.

9. Appendix B

Breach Management Plan

There are four important elements to any breach management plan:

- Containment and recovery
- Assessment of ongoing risk
- Breach notification
- Evaluation and response

Containment and recovery

Data security breaches will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. This will often involve input from specialists across the school, such as IT, HR and legal and, in some cases, contact with external stakeholders and suppliers.

The following needs to be considered:

- Decide on who should take the lead on investigating the breach and ensure they have the appropriate resources.
- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This could be isolating or closing a compromised section of the network, finding a lost piece of equipment or simply changing the access codes at the front door.
- Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause. As well as the physical recovery of equipment, this could involve the use of back ups to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data.
- Where appropriate, inform the police where there is evidence to indicate a crime has taken place.
- Where appropriate, consider reporting a personal data breach to the ICO.

Assessment of ongoing risks

Before deciding on what steps are necessary following immediate containment, assess the risks which may be associated with the breach. The following points are also likely to be helpful in making this assessment:

- What type of data is involved?
- How sensitive is it?
- If data has been lost or stolen, are there any protections in place such as encryption?
- Regardless of what has happened to the data, what could the data tell a third party about the individual?
- How many individuals' personal data are affected by the breach?
- Who are the individuals whose data has been breached? Whether they are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach and, therefore, your actions in attempting to mitigate those risks.
- What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

Breach notification

Mandatory reporting to the ICO

- Under GDPR, Norwood Green Junior School is required to notify the ICO of a breach where it is likely to result in a 'high risk' to the rights and freedoms of individuals.
- Whether there is such a risk is also likely to vary depending on the type of data that is the subject of the breach and the type of breach that has occurred. A breach that is likely to have a significant detrimental effect on individuals, e.g. disclosure of an individual's health or financial information, may be likely to have a significantly higher risk to the rights and freedoms of a data subject than a breach that leads to disclosure of individual's names with no further information about the individuals.
- This must be assessed on a case-by-case basis. For example, the school will need to notify the ICO about a loss of pupil/parent details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.
- The severity of the personal data breach/incident will be determined by the scale (numbers of data subjects affected) and sensitivity factors selected. If the outcome in terms of the severity of the incident is Level 2 (reportable), the incident should be reported to the ICO and escalated to other regulators, as appropriate. Please refer to Annex A – Incident Severity Assessment, which will help determine whether an incident is externally reportable.
- Although the primary factors for assessing the severity level are the numbers of individual data subjects affected, the potential for media interest, and the potential for reputational damage, other factors may indicate that a higher rating is warranted, for example the potential for litigation or significant distress or damage to the data subject(s) and other personal data breaches of the GDPR. As more information becomes available, the personal data breach should be re-assessed. Where the numbers of individuals that are potentially impacted by an incident are unknown, a sensible view of the likely worst case should inform the assessment of the incident. When more accurate information is determined, the level should be revised as quickly as possible.

  Please note: No reporting is required if the breach is unlikely to result in a risk to the rights and freedoms of natural persons. For example, when lost data is protected, e.g. by appropriate encryption, so that no individual's data can be accessed, then there is no data breach. When the data is protected but risk of individuals being identified remains, an incident should be reported.

Timing

- Where a personal data breach is deemed reportable to the ICO, it must be reported without undue delay and, where feasible, not later than 72 hours after becoming aware of it.
- Where a notification is not made within 72 hours of the data breach, Norwood Green Junior School must give a 'reasoned justification' to the ICO explaining the reason for the delay.
- The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide information in phases. In practice, notification to the ICO may be required initially, followed by an in-depth analysis of the incident.

Communicating personal data breaches to individuals affected

- If the breach is sufficiently serious to warrant notification to the public, Norwood Green Junior School will do so without undue delay.

- Informing pupils, parents and staff that the school has experienced a data security breach is an important element in Norwood Green Junior School's breach management strategy. Considering the following will assist in deciding whether and how to notify:
  - Can notification help the individual? Bearing in mind the potential effects of the breach, could individuals act on the information you provide to mitigate risks, for example by being able to monitor any unusual or suspicious bank transactions, checking their credit rating, cancelling a credit card or changing a password?
  - If a large number of people are affected, or there are very serious consequences, the school should inform the ICO.
  - Consider how notification can be made appropriate for particular groups of individuals, for example, if notifying children or vulnerable adults.
  - Consider the dangers of 'over notifying'? Not every incident will warrant notification.
  - Consider who to notify, what you are going to tell them and how you are going to communicate the message. The notification should at the very least include a description of how and when the breach occurred and what data was involved. Include details of what has already been done to respond to the risks posed by the breach.
  - When notifying individuals give specific and clear advice on the steps they can take to protect themselves and also what the school is willing to do to help them. For example, the school may wish to pay for annual subscription to a credit reference agency where financial data may have been compromised.
  - Provide a way in which they can contact the school for further information or to ask questions about what has occurred.

There are, however, some circumstances when the notification to the data subject is not required, including:

- Where the school has implemented appropriate technical and organisational protection measures in respect of the personal data affected by the breach (such as encryption).
- Where the school has taken subsequent measures which ensure that the high risk to the rights and freedoms of individuals is no longer likely to arise.
- When it would involve disproportionate effort. A public notice or similar would be required to communicate the breach in those circumstances.

The ICO may compel Norwood Green Junior School to communicate a personal data breach with affected data subjects/individuals unless one of the three exemptions listed above is satisfied.

Evaluation and response

It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of the response to it. Clearly, if the breach was caused, even in part, by systemic and ongoing problems, then simply containing the breach and continuing 'business as usual' is not acceptable; similarly, if the response was hampered by inadequate policies or a lack of a clear allocation of responsibility, then it is important to review and update these policies and lines of responsibility in light of the experience.

Incident severity assessment

Not all incidents have the same potential to adversely impact on the individuals whose data are involved. Assessing the severity of an incident relies on several factors, and there is no simple definition that covers what a serious incident entails. An incident that appears to be of minor importance may, on further investigation, be found to be serious and vice versa.

Although the full extent of an incident is only known after it has been thoroughly investigated, there is a need to ascertain whether the risk could be classified as serious at an early stage.

The crucial factors for assessing the severity level of an incident are:

- the number of individual data subjects (pupils, staff and parents) affected

- the potential for significant distress or damage to the data subject
- the potential for reputational damage to Norwood Green Junior School
- the potential for litigation
- the potential for media interest
- the type of personal data breach. Data breaches affecting special categories of data are more sensitive, and thus need to be treated more seriously than data breaches of personal data (refer to Appendix D for a complete list of what constitutes special categories of data).

Loss or theft of encrypted removable media (laptops, CDs, USB memory sticks, media cards, Personal Digital Assistants (PDAs)) would not constitute a reportable incident unless there is reason to believe that the protection afforded by these devices has been compromised, e.g. the key(s) used to unencrypt have also been compromised, the laptop was not configured to automatically enforce account lockout after a short time lapse without user interaction.

There are two factors which influence the severity – scale and sensitivity.

Scale factors

While any personal data breach is potentially a very serious matter, the number of individuals that might potentially suffer distress, harm or other detriment is clearly an important factor. The scale (as demonstrated in Table 1 below) provides the base categorisation level of an incident, which will be modified by a range of sensitivity factors.

Sensitivity factors

Sensitivity in this context may cover a wide range of different considerations and each incident may have a range of characteristics, some of which may raise the categorisation of an incident and some of which may lower it. The same incident may have characteristics that do both, potentially cancelling each other out. For the purpose of the incident, sensitivity factors may be:

- Low: Reduces the base categorisation
- High: Increases the base categorisation.

<u>Categorising Personal Data Breaches</u>

The incident category is determined by the context, scale and sensitivity. Every incident can be categorised as:

- Level 0 or 1: Confirmed incident but no need to report to ICO and other regulators.
- Level 2 or above: Confirmed incident that must be reported to ICO and other regulators.

To determine which category your incident falls under, first use Table 1 to identify the baseline category for the breach, based on the scale of the incident, then use Table 2 to determine the final category, based on the sensitivity of the incident.

Table 1: Baseline category based on scale of incident

Baseline category	Definitions
0	Information about less than 10 individuals
1	Information about 11–50 individuals
1	Information about 51–100 individuals
2	Information about 101–300 individuals
2	Information about 301–500 individuals
2	Information about 501–1,000 individuals

3	Information about 1,001–5,000 individuals
3	Information about 5,001–10,000 individuals
3	Information about 10,001–100,000 individuals
3	Information about 100,001 + individuals

Table 2 – Category changes based on sensitivity

Scores	Sensitivity characteristics
+1 FOR EACH CHARACTERISTIC	Sensitive categories of data (Appendix D)
	Detailed information at risk, e.g. financial information
	One or more previous incidents of a similar type in past 12 months
	Failure to securely encrypt mobile technology or the other obvious security failing
	media interest
	A complaint has been made to the ICO
	Individuals affected have been placed at risk of physical harm
	Individuals affected may suffer significant detriment, e.g. financial loss
	Individuals affected are likely to suffer significant distress or embarrassment
-1 FOR EACH CHARACTERISTIC	No data at risk
	Limited demographic data at risk, e.g. address not included, name not included
	Security controls/ difficulty to access data partially mitigates risk

Table 3 – Incident reporting requirements

Final score	Level of incident
1 OR LESS	Level 1 incident (to be reported internally)
2 OR MORE	Level 2 incident (to be reported to the ICO, and internally)

Notification of data breaches to the ICO

There are also prescribed requirements under the GDPR to satisfy when communicating a breach to the ICO. Guidance from the ICO regarding reporting of incidents is detailed in the list below and included in the Incident Report Form Template in Appendix B.

Information should include:

- Norwood Green Junior School contact details, stating Norwood Green Junior School is the Data Controller in respect of the data breach
- the Data Controller registration number, although under the GDPR this will no longer be a mandatory requirement
- contact details of person in charge of the incident: name, job title, email address, contact telephone number and postal address
- the reason(s) for any delay(s) in notifying, if applicable
- measures the organisation have in place to prevent an incident of this nature occurring
- extracts of relevant policies and procedures
- what personal data has been placed at risk
- number of individuals affected and approximate number of data records concerned
- whether the affected individuals have been made aware of this breach

- the potential adverse effects on those individuals
- any palliative measures taken
- whether the data placed at risk has been recovered
- evidence of existing staff training, including relevant excerpts, and whether it is mandatory
- any previous incidents that had been reported to the ICO, providing a succinct summary.

This information is to be sent to casework@ico.org.uk, with 'DPA breach notification form' in the subject field, or by post to: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

The ICO will issue an initial response within seven calendar days and provide a case reference number and information about their next steps.

Furthermore, Norwood Green Junior School has a duty to inform Data Subjects whether there is potential for identity theft which can be avoided or minimised if the Data Subject is notified of the incident, without undue delay.

Failing to comply with the notification requirement under the GDPR means Norwood Green Junior School will potentially attract GDPR fines, such as €20 million, or 4% of the company's annual global turnover, whichever is higher.

Incident management

An individual must be assigned to manage the incident, and will be responsible for communicating and coordinating activities, as well as maintaining an audit trail of events and evidence. An investigation needs to be conducted to determine the causes of the breach, the scope, and possible remediation, along with expected outcomes and the identification of stakeholders. Evidence is to be preserved in order of volatility.

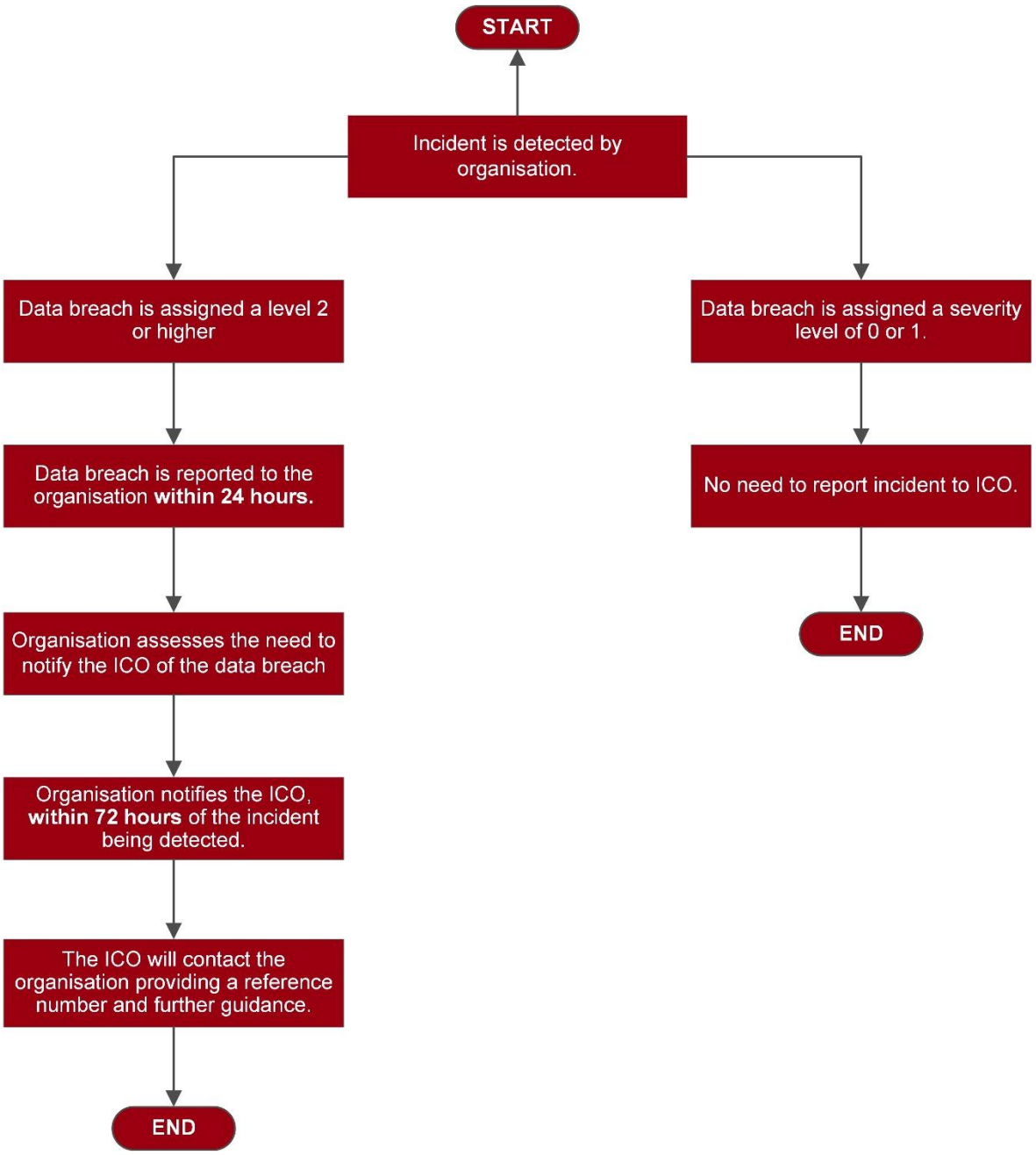
Following the investigation, mitigation and preventative measures must be documented and put in place, and a final incident report produced to obtain a sign-off from the Norwood Green Junior School Trustees.

Personal data breach register

Under the GDPR, both Data Controllers and Data Processors are required to record any personal data breaches and any actions taken in respect of that. An Internal Breach Register will be maintained, documenting each incident 'comprising the facts relating to the personal data breach, its effects and the remedial action taken'.

The ICO has the authority to assess how Norwood Green Junior School complies with its data breach notification obligations.

Incident management flow diagram



Norwood Green Junior School

ICO Incident Report Form

ICO INCIDENT REPORT FORM		
Date	Time	Location
Organisation name		
Name of person reporting incident		
Job title		
Phone number		
Postal address		
Email address		
Description of incident		
Reason for delaying notification, if applicable		
Number of people affected		
Volume of data affected		
Measures Norwood Green Junior School has in place to deal with such incidents		
Potential adverse effects on individuals affected		
Mitigating measures taken		
Have the data been recovered?		
Has Norwood Green Junior School reported data breaches to the ICO in the past? If yes, provide details.		

Norwood Green Junior School

Internal Incident Report Form

INTERNAL INCIDENT REPORT FORM		
Date	Time	Location
Name of person reporting incident		
Job title		
Phone number		
Email address		
Description of incident		
Level of incident		
Number of people affected		
Volume of data affected		
Data format (paper/electronic)		
If electronic, are records encrypted?		
Is the incident in the public domain?		
Is the media aware of the incident?		
Immediate action taken		
Remedial action taken		
For Norwood Green Junior School use		
Incident reference number		
Received by		
Forwarded for action to		
Remedial action taken		

Norwood Green Junior School

Special Categories of Data Overview

Racial or ethnic origin of the data subject
Political opinions
Religious beliefs or other beliefs of a similar nature
Trade union membership
Physical or mental health condition
Sexual life
The commission or alleged commission by the individual of any offence
Any proceedings for any offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in such proceedings
Biometric or genetic data

10. Appendix C

Individual Rights

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

The GDPR does not specify how an individual makes a valid request to the list above. Therefore, an individual can make a request verbally or in writing. It can also be made to any part of the school organisation and does not have to be to a specific person or contact point.

A request in relation to personal data does not need to mention the specific area of right/requirement. As long as the individual has asked that the school take steps this will be a valid request.

This presents a challenge as any of our employees could receive a valid verbal request. However, the school has a legal responsibility to identify that an individual has made a request to us and handle it accordingly. Will we therefore ensure that staff are aware that any individual making a request should be directed to the school office.

As good practice the school will record details of the requests it receives, particularly those made by telephone or in person. This will allow the school to check with the requester that we have understood their request. This can help avoid later disputes about how we have interpreted the request. We will also keep a log of verbal requests.

If the school has doubts about the identity of the person making the request we will ask for more information. We will only request information that is necessary to confirm who they are.

The school will let the individual know without undue delay and within one month that we need more information from them to confirm their identity.

<u>The right to be informed</u>

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.

The school provides individuals with information including: the purposes for processing their personal data, the retention periods for that personal data, and who it will be shared with. This is provided to individuals through the school's Privacy Notice to parents/carers and employees.

If Norwood Green Junior School obtains personal data from other sources, it must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.

There are a few circumstances when the school does not need to provide people with privacy information, such as if an individual already has the information or if it would involve a disproportionate effort to provide it to them.

The information the school provides to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.

The right of access

Individuals have the right to confirm that their data is being processed, access to their personal data and other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

Norwood Green Junior School will provide a copy of the information **free of charge**. However, we can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

The school may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that we can charge for all subsequent access requests.

The fee will be based on the administrative cost of providing the information.

Information will be provided without delay and at the latest within one month of receipt. The one month response deadline starts from the day the request is received, rather than the day after. For example, a SAR received on 3rd September should be responded to by 3rd October.

The school will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, the school will inform the individual within one month of the receipt of the request and explain why the extension is necessary. If the school needs to process a large amount of information about an individual, the school may be able to ask them to specify the information or processing activities their request relates to, if it is not clear. The time limit for responding to the request is paused until the school receives clarification, although the school should supply any of the supplementary information it can do within one month.

Where the school refuses to respond to a request, we will explain why to the individual, informing them of their right to complain to the ICO and that they can seek to enforce their subject access right through the courts without undue delay and at the latest within one month.

The school does not have to confirm whether we hold the requested data.

Reasons for Refusal:

Unfounded or excessive requests

Requests that are "manifestly unfounded or excessive" can be refused. This might be where a request is repetitive or asks for further copies of the same previously supplied information. If the school decides to fulfil such a request, we can charge a reasonable fee to comply, based on the administrative cost of providing the information. The school will need to contact the requester promptly to inform them of the fee, and wouldn't need to comply with the request until payment is received.

Concerns about "serious harm"
The school can refuse requests for certain pieces of data if we believe they meet the "serious harm" test, meaning sharing the information would be likely to cause serious harm to the physical or mental health of any individual.

This applies to:

- Education data (i.e. personal data kept in educational records)
- Social work data

Similarly, we can refuse requests for child abuse data from anyone with parental responsibility for a pupil if sharing the data would "not be in the best interests" of their child. This will cover any information as to whether a child is or has been the subject of child abuse or may be at risk of it.

Conversely, the school should not share any health data via a request unless, within the last 6 months, we have been told by an appropriate health professional that the serious harm test is **not** met.

Even if we have been informed of this in the last 6 months, we must re-consult with the appropriate health professional about this if it would be reasonable to do so.

Information that includes others' personal data
The school does not have to comply with a request for information that includes personal data about an individual other than the requester or their child, except if:

- The other individual has consented to the disclosure; or
- It's reasonable to comply with the request without that individual's consent

In determining whether it is reasonable to disclose the information, the school should take into account the relevant circumstances such as:

- The type of information that would be disclosed
- Any duty of confidentiality owed to the other individual
- Any steps taken to seek consent from the other individual
- Whether the other individual is capable of giving consent
- Any express refusal of consent by the other individual

The school should consider as well whether it can redact or change the format of the data so the other individual is suitably anonymised.

It is considered reasonable to disclose information about 'education-related' workers at school without consent so long as the information relates to their employment. For example, if we receive a request for a pupil report written by a teacher, we would not need to redact the teacher's name or seek consent from them to share the report.

Other exemptions
Other types of personal data the school can refuse to share with a requester, such as information related to:

- Crime, if disclosing the personal data would be likely to prejudice the prevention or detection of crime, or the apprehension and prosecution of offenders
- Immigration, if disclosing the personal data would prejudice the maintenance of effective immigration control

- Legal professional privilege - check with a legal expert if the school is not sure whether this privilege applies
- Management forecasts, such as planned redundancies or restructuring
- Negotiations, such as if you are negotiating about a pay rise or promotion
- Confidential references, regardless of whether you have sent or received such a reference

The right to rectification

The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete.

- An individual can make a request for rectification verbally or in writing.
    - The school has one calendar month to respond to a request. This can be extended to 2 months where the request is complex.
- In certain circumstances the school can refuse a request for rectification.
- This right is closely linked to the controller's obligations under the accuracy principle of the GDPR (Article (5)(1)(d)).

If the school receive a request for rectification the school will take reasonable steps to satisfy itself that the data is accurate and to rectify the data if necessary. We will take into account the arguments and evidence provided by the data subject.

What steps are reasonable will depend, in particular, on the nature of the personal data and what it will be used for. The more important it is that the personal data is accurate, the greater the effort the school will put into checking its accuracy and, if necessary, taking steps to rectify it. For example, the school will make a greater effort to rectify inaccurate personal data if it is used to make significant decisions that will affect an individual or others, rather than trivial ones.

The school may also take into account any steps it has already taken to verify the accuracy of the data prior to the challenge by the data subject.

If the data in question records a disputed opinion, it can be difficult to conclude that the record of an opinion is inaccurate. The school will ensure that the record shows clearly that the information is an opinion and, where appropriate, whose opinion it is.

If the school is satisfied that the data is accurate, we will let the individual know and tell them that the school will not be amending the data. The school will explain its decision, and inform the individual of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce their rights through a judicial remedy.

As good practice the school will place a note on its system indicating that the individual challenges the accuracy of the data and their reasons for doing so.

The right to erasure/be forgotten

Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which the school originally collected or processed it for;
- the school is relying on consent as its lawful basis for holding the data, and the individual withdraws their consent;
- the school is relying on legitimate interests as its basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- the school is processing the personal data for direct marketing purposes and the individual objects to that processing;
- the school has processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);
- the school has to do it to comply with a legal obligation; or
- the school has processed the personal data to offer information services to a child.

There is an emphasis on the right to have personal data erased if the request relates to data collected from children. This reflects the enhanced protection of children's information, especially in online environments, under the GDPR.

Therefore, if we process data collected from children, the school will give particular weight to any request for erasure if the processing of the data is based upon consent given by a child – especially any processing of their personal data on the internet. This is still the case when the data subject is no longer a child, because a child may not have been fully aware of the risks involved in the processing at the time of consent.

The school can refuse to erase a data subject's personal data where it is processed:

- to exercise a right of freedom of expression and information;
- to comply with a legal obligation or for the performance of a task of public interest;
- for the exercise or defence of legal claims; or
- for purposes relating to public health, archiving in the public interest, scientific/historic research or statistics.

The school will tell other organisations about the erasure of personal data if:

- the personal data has been disclosed to others; or
- the personal data has been made public in an online environment (for example on social networks, forums or websites).

The right to restrict processing

Individuals have the right to request the school restrict the processing of their personal data in the following circumstances:

- the individual contests the accuracy of their personal data and we are verifying the accuracy of the data;

- the data has been unlawfully processed and the individual opposes erasure and requests restriction instead;
- the school no longer need the personal data but the individual needs us to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to the school processing their data under Article 21(1), and we are considering whether our legitimate grounds override those of the individual.

As a matter of good practice the school will automatically restrict processing whilst considering its accuracy or the legitimate grounds for processing the personal data in question.

Once the school has made a decision on the accuracy of the data, or whether our legitimate grounds override those of the individual, we may decide to lift the restriction.

If the school does this, we will inform the individual **before** lifting the restriction.

The right to data portability

The right to data portability allows data subjects to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. It also gives them the right to request that a controller transmits this data directly to another controller.

The right to data portability only applies when:

- the school's lawful basis for processing this information is consent **or** for the performance of a contract
- the school is carrying out the processing by automated means (ie excluding paper files).

If the requested information includes information about others (eg third party data) the school needs to consider whether transmitting that data would adversely affect the rights and freedoms of those third parties.

If the requested data has been provided to the school by multiple data subjects (eg a joint bank account) we need to be satisfied that all parties agree to the portability request. This means that we may have to seek agreement from all the parties involved.

The school will provide the personal data in a structured, commonly used and machine readable form (e.g. CSV files).

If the individual requests it, the school may be required to transmit the data directly to another organisation if this is technically feasible.

The school will comply with the data subject's request free of charge and within one month. This can be extended to 2 months where the request is complex or if we receive a number of requests.

The school can refuse to comply with a request for data portability if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature or request a reasonable fee to deal with the request.

The school will base the reasonable fee on the administrative costs of complying with the request. If we decide to charge a fee we will contact the individual promptly and inform them. The school does not need to comply with the request until we have received the fee.

If the school refuses to comply with a request for data portability, we will inform the individual without undue delay and within one month of receipt of the request about:

- the reasons we are not taking action;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

The right to object

Article 21 of the GDPR gives individuals the right to object to the processing of their personal data. This effectively allows individuals to ask the school to stop processing their personal data.

The right to object only applies in certain circumstances. Whether it applies depends on the school's purposes for processing and our lawful basis for processing.

Individuals have the absolute right to object to the processing of their personal data if it is for direct marketing purposes.

Individuals can also object if the processing is for:

- a task carried out in the public interest;
- the exercise of official authority vested in the school; or
- the school's legitimate interests (or those of a third party).

In these circumstances the right to object is not absolute.

If one of these conditions applies, the school will explicitly bring the right to object to the individual's attention. This information will be presented clearly and separately from any other information.

Direct marketing

An individual can ask the school to stop processing their personal data for direct marketing at any time. This includes any profiling of data that is related to direct marketing.

This is an absolute right and there are no exemptions or grounds for the school to refuse. Therefore, if the school receives an objection to processing for direct marketing, we will stop processing the individual's data for this purpose.

The school will not erase the individual's personal data but will suppress their details, which will involve retaining just enough information about them to ensure that their preference not to receive direct marketing is respected in future.

Processing based upon public task or legitimate interests

An individual can also object where the school is relying on one of the following lawful bases:

- 'public task' (for the performance of a task carried out in the public interest),
- 'public task' (for the exercise of official authority vested in you), or
- legitimate interests.

An individual must give specific reasons why they are objecting to the processing of their data. These reasons should be based upon their particular situation.

In these circumstances this is not an absolute right, and the school can continue processing if:

- we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

The school will consider the reasons why they have objected to the processing of their data when we are deciding whether we have compelling legitimate grounds which override the interests of an individual.

If the school is satisfied that we do not need to stop processing the personal data in question the school will let the individual know explaining our decision, and inform them of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce their rights through a judicial remedy.

The school can also refuse to comply with an objection if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature or can request a reasonable fee to deal with the request.

In either case the school will need to justify its decision.

The school will inform the individual without undue delay and within one month of receipt of the request:

- reasons the school are not taking action;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

Rights relating to automated decision making and profiling

"Profiling" is any form of automated processing intended to evaluate certain personal aspects of a data subject, in particular to analyse or predict their performance at work, economic situation, health, personal preferences, reliability, behaviour and location.

Data subjects have the right not to be subject to a decision when:

- it is based on automated processing; and

- it produces a legal effect or a similarly significant effect on the individual.

The school must ensure data subjects are able to:

- obtain human intervention;
- express their point of view; and
- obtain an explanation of the decision and challenge it.

The above right does not apply if the automated decision:

- is necessary for entering into or performance of a contract between the school and the individual;
- is authorised by law (e.g. for the purposes of fraud or tax evasion prevention);
- is based on explicit consent; or
- does not have a legal or similarly significant effect on the data subject.

When processing personal data for profiling purposes, the school will ensure that appropriate safeguards are in place. For example:

- being fair and transparent about the logic involved;
- using appropriate mathematical/statistical procedures;
- implementing appropriate technical and organisational measures to correct inaccuracies and minimise the risk of errors; and
- keeping personal data secure in a proportionate way

The school will avoid making automated decisions based on sensitive personal data unless we have the explicit consent of the data subject or have reasons of substantial public interest.

Because this type of processing is considered to be high-risk the school will carry out a Data Protection Impact Assessment (DPIA) to show that we have identified and assessed what those risks are and how we will address them if it enters into automated decision making and profiling.