Hillside Primary School

Data Protection Policy

If you are reading a printed version of this document, you should check the school website to ensure that you have the most up-to-date version.

If you would like to discuss anything in this data protection policy, please contact:

Data Protection Officer: **Data Protection Education Ltd.**

Telephone: 0800 0862018

Email: dpo@dataprotection.education

If you would like a copy of any documentation, please contact the school office: **office@hillside.norfolk.sch.uk**

Contents

1. COMMITMENT TO GENERAL DATA PROTECTION AND DATA PROTECTION BY DESIGN 4
2. POLICY OBJECTIVES, ROLES & RESPONSIBILITIES 5
3. POLICY STATEMENT 5
4. ABOUT THIS POLICY 6
5. DATA PROTECTION OFFICER 6
6. DATA PROTECTION PRINCIPLES 7
7. DATA SUBJECT'S RIGHTS 8
8. FAIR AND TRANSPARENT PROCESSING OF DATA 9
9. LAWFUL PROCESSING OF DATA 10
10. SPECIAL CATEGORY DATA 10
11. CONSENT 11
12. DISCLOSURE AND SHARING OF PERSONAL INFORMATION 12
13. DATA SECURITY 12
14. DATA PROTECTION IMPACT ASSESSMENTS 13
15. DATA BREACHES 14
16. SUBJECT ACCESS REQUESTS 15
17. PUBLICATION OF INFORMATION 16
18. DBS DATA 16
19. PHOTOGRAPHY IMAGES AND VIDEOS 17
20. RETENTION POLICY 18
21. TRAINING 18
22. DATA PROCESSORS 18
23. CHANGES TO THIS POLICY 19

APPENDIX DEFINITIONS 20

APPENDIX 2. EXAMPLES OF DATA BREACHES 23

APPENDIX 3. DEALING WITH SUBJECT ACCESS REQUESTS 24

1. COMMITMENT TO GENERAL DATA PROTECTION AND DATA PROTECTION BY DESIGN

1.1. Data Protection Act 2018 (DPA) is the law that protects personal privacy and upholds individual rights in relation to data protection. It applies to anyone who handles or has access to people's personal data.

1.2. This policy is intended to ensure that personal information is dealt with appropriately and securely, in accordance with this legislation. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

1.3. This policy sets out the organisation's commitment to data protection and the implementation of a data protection by design approach.

1.4. The organisation will refer to documents and guidance from the Information Commissioner's Office and the Department for Education in relation to data protection and data processing.

1.5. This includes ensuring the following:

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

2. POLICY OBJECTIVES, ROLES & RESPONSIBILITIES

2.2. **The organisation, as the Data Controller,** will comply with its obligations under The Protection Act 2018. The organisation is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rights under the legislation. This policy sets out how the organisation will do this.

2.2. All organisation staff and organisation workforce must have a general understanding of the law and understand how it may affect their decisions to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this policy to comply with its obligations under UK GDPR and the Data Protection Act 2018.

2.3. **The Information Commissioner as the Regulator** can impose substantial fines for breaches of UK GDPR and the Data Protection Act 2018, and other Data Protection Legislation. Therefore, it is imperative that the organisation, all staff and the workforce comply with the legislation. The Data Protection Officer will be the principal point of contact with the ICO.

3. POLICY STATEMENT

3.1 Everyone has rights with regards to the way in which their personal data is handled. During our activities as an organisation, we will collect, store and process personal data about our pupils, workforce, parents and others. This makes us a data controller in relation to that personal data.

3.2 We are committed to the protection of all personal data and special category personal data for which we are the data controller.

3.3 The law imposes significant fines for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in those fines being applied.

3.4. All members of our staff and workforce will comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action.

4. ABOUT THIS POLICY

4.1. The types of personal data that we may be required to handle include information about pupils, parents, our workforce, and others that we deal with. The personal data which we hold is subject to certain legal safeguards specified in The Data Protection Act 2018, and other Data Protection Legislation

4.3. This policy does not form part of any employee's contract of employment and may be amended at any time.

4.4. This policy sets out rules on data protection and the legal conditions that must be satisfied when the organisation processes personal data.

4.2. This policy, combined with the organisation's privacy policy and any other document referred to herein, sets out the basis on which the organisation will process any personal data collected from data subjects or provided to us by data subjects directly and or from other sources.

5. DATA PROTECTION OFFICER

5.1. As an organisation, we are required to appoint a Data Protection Officer ("DPO"). **Our DPO is Data Protection Education,** and they can be contacted at dpo@dataprotection.education

The DPO is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

5.2. The organisation shall maintain a Data Protection Officer to represent the rights of data subjects and a named Data Protection lead in order to assist the Data Protection Officer.

5.3. The organisation shall ensure that the Data Protection Officer is involved properly and in a timely manner, in all issues which relate to the protection of personal data.

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

5.5. The organisation shall ensure that the Data Protection Officer does not receive any instructions regarding the exercise of their tasks. They shall not be dismissed or penalised by the controller or the processor for performing their tasks.

5.6 The Data Protection Officer shall directly report to the highest management level of the organisation, as needed and report to the Board of Governors at least once a year.

5.7. Data subjects may contact the Data Protection Officer with regards to all issues related to the processing of their personal data and to the exercise of their rights under the regulations.

5.8. The Data Protection Officer and the Data Protection Lead will be bound by confidentiality and must maintain data security by protecting the confidentiality**,** integrity and availability of all personal data, defined as follows:

- **Confidentiality** means that only people who have a need to know and are authorised to use 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 only authorised users can access personal data when they need it for authorised purposes.

5.9. The Data Protection Officer shall have the following responsibilities:

- Review of all data processing activities (inventory/mapping).
- Conduct of regular health checks/audits and issue recommendations.
- Assist with data protection impact assessments and monitoring performance.
- Monitoring and advice relating to subject access requests and data breaches.
- Assist the organisation with the maintenance of records.
- Monitoring and advice relating to FOI and other information requests.
- Cooperation with and acting as the contact point for the Information Commissioner's Office, which is the supervisory authority in respect of all data protection matters.
- Act as the contact point for data subjects to deal with requests and complaints.
- Training of organisation staff and workforce.

6. DATA PROTECTION PRINCIPLES

6.1. Anyone processing personal data must comply with the data protection principles. The organisation will comply and is committed to these principles in relation to any processing of personal data. The Data Protection principles provide that personal data must be:

- **Processed lawfully, fairly and in a transparent manner** in relation to the data subject and their rights;
- **Collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes;
- **Adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed;
- **Accurate and, where necessary, kept up to date;**
- **Kept in a form which permits identification of data subjects for no longer than is necessary**;
- **Processed in a manner that ensures appropriate security of the personal data; and**
- **Must NOT be transferred to people or organisations situated in other countries without adequate protection.**

7. DATA SUBJECT'S RIGHTS

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

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

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

8. FAIR AND TRANSPARENT PROCESSING OF DATA

8.1. Data Protection Legislation is not intended to prevent the processing of personal data but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

8.2. For personal data to be processed fairly, data subjects must and will be made aware of the following in our privacy notices or requests to process data:

- That the personal data is being processed;
- Why the personal data is being processed;
- What the lawful basis is for that processing (see below);
- Whether the personal data will be shared, and if so, with whom;
- The period for which the personal data will be held;
- The existence of the data subject's rights in relation to the processing of that personal data; and
- The right of the data subject to raise a complaint with the Information Commissioner's Office in relation to any processing.

8.3. The organisation will only process data that is **necessary and relevant to the purpose for which it was gathered and will ensure that we have a lawful basis for any processing.**

8.4 Data collected for the purposes of public health (including visitor contact data for COVID-19) will be kept as long as required. Contact data for visitors will be kept for 21 days after the most recent visit, with information on visitors kept as per standard retention requirements. Public Health data may be shared with third parties as required, including, but not limited to:

- National Health Service (including NHS Test and Trace)
- Public Health England
- Other local health authorities

Data collected and processed for public health purposes is done so under GDPR Article 9(2)(i) which states: (in part) "processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health..." and Recital 54 which includes: "The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject."

8.5 Collection and processing of visitor data will be documented in the privacy notices and in a statement available to visitors at the time of data collection to include the following information:

"We collect the following visitor information for the purposes of security, safety and public health:

- Name
- Organisation
- Date and time of visit
- Car registration (when parked on school premises)
- Contact details

These are kept for six years in case of any claims by students, staff or visitors under the Limitations Act (1980).

9. LAWFUL PROCESSING OF DATA

9.1. For personal data to be processed lawfully, it must be processed on the basis using one of the legal grounds set out in the Data Protection Legislation. The organisation will only process personal data where a lawful basis for processing exists. Specifically, where:

- The data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;
- Processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- Processing is necessary for compliance with a **legal obligation** to which the controller is subject (e.g the Education Act 2011);
- Processing is necessary in order to protect the **vital interests** of the data subject or of another natural person;
- Processing is necessary for the **performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller.

10. SPECIAL CATEGORY DATA

10.1. This is data relating to **health; race; sexuality; religion; criminal offences; political opinions and union memberships**.

10.2. These special categories of personal data relating to will not be processed unless a specific lawful basis, as listed in Article 9 of the UK GDPR applies. When this special category data is being processed, we will normally only do so under the following legal grounds:

- Where the processing is **necessary for employment law** purposes, for example, in relation to sickness absence;
- Where the processing is necessary for reasons of substantial public interest, for example, for the purposes of equality of opportunity and treatment;
- Where the processing is necessary for **health or social care purposes**, for example, in relation to pupils with medical conditions or disabilities; and
- **Where none of the above applies then we will seek the consent of the data subject to the processing of their special category personal data.**

11. CONSENT

11.1. There are strict legal requirements in relation to the form of consent that must be obtained from data subjects.

11.2. When pupils, staff or our Workforce join the Organisation a consent form will be required to be completed in relation to them. This consent form deals with for example: school displays, school website, social media and external publications etc.

11.3. Where appropriate third parties may also be required to complete a consent form.

11.4. In relation to all pupils under the age of 12 years old, we will seek consent from an individual with parental responsibility for that pupil.

11.5. We will generally only seek consent directly from a pupil if they are legally able to give such consent. The legal age for consent under Data Protection legislation is 12. However, we recognise that this may not be appropriate in certain circumstances and therefore, the organisation may be required to seek consent from an individual with parental responsibility.

11.6. If consent is required for the processing of personal data of any data subject, then the form of this consent must:

- Inform the data subject of exactly what we intend to do with their personal data;
- Require them to positively confirm that they consent (we cannot ask them to opt-out rather than opt-in); and
- Inform the data subject of how they can withdraw their consent.

11.7. Any **consent must be freely given**, which means that we cannot make the provision of any goods or services or other matter conditional on a data subject giving their consent.

11.8. The DPO must always be consulted in relation to any consent form before consent is obtained.

11.9. A record must always be kept of any consent, including how it was obtained and when.

11.10. There may be circumstances where it is considered necessary to process personal data or special category personal data to protect the vital interests of a data subject. This might include safeguarding, child protection and medical emergencies where the data subject is not able to give consent to the processing. We believe that this will only occur in very specific and limited circumstances. In such circumstances, we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur. Please refer to the organisation's Safeguarding Policy, Child Protection Policy and organisation Medical Policy for further information.

12. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

12.1. We may share personal data that we hold about data subjects, with other organisations, without consent where we have a lawful basis for doing so. Such organisations include the Department for Education and Education and Skills Funding Agency "ESFA", Ofsted, health authorities and professionals, the Local Authority, examination bodies, other organisations, and other organisations where we have a lawful basis for doing so.

12.2 The organisation will inform data subjects of any sharing of their personal data unless we are not legally required to do so, for example, where personal data is shared with the police in the investigation of a criminal offence.

12.3 In some circumstances, we will not share safeguarding information. Please refer to our Child Protection Policy.

12.4 Further detail is provided in our Record of Processing Activities.

13. DATA SECURITY

13.1. The organisation will implement appropriate data security measures using policies, procedures and technologies to ensure and maintain the security of all personal data from the point of collection to the point of destruction.

13.2. These security measures will be appropriate to the risks in processing personal data and will be consistent with the rights of the data subjects.

13.3. These measures shall include as appropriate:

- Measures and data access controls to ensure that the Personal Data can only be accessed by authorised personnel for the purposes agreed in the record of processing activity and outlined in the organisation privacy notice;
- In assessing the appropriate level of security account shall be taken in particular of all the risks that are presented by processing, for example from accidental or unlawful destruction, loss, or alteration, unauthorised or unlawful storage, processing, access or disclosure of personal data;
- The anonymisation, pseudonymisation and encryption of personal data;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- A process for regular testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing of personal data;
- Measures to identify vulnerabilities with respect to the processing of personal data in systems used to provide services to The Organisation.
- Adherence to an Acceptable Use Policy when using technology to ensure the security and confidentially of personal data when using all systems (including email) in all environments across the organisation.
- Care should be taken whilst reading emails, messages or notifications to prevent them being read by unauthorised persons.
- Email classification should be in place, and emails flagged (or described in the subject line) as "Sensitive/Highly Sensitive" when appropriate.

14. DATA PROTECTION IMPACT ASSESSMENTS

14.1. The organisation takes data protection very seriously and will consider and comply with the requirements of Data Protection Legislation in relation to all of its activities, whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

13.2. In certain circumstances, the law requires us to carry out detailed assessments of proposed processing. This includes where we intend to use new technologies which might pose a high risk to the rights of data subjects because of the types of data we will be processing or the way that we intend to do so.

14.3. The organisation will complete an assessment of any such proposed processing and will use a template document which ensures that all relevant matters are considered.

14.4. The DPO should always be consulted as to whether a data protection impact assessment is required and, if so, how to undertake that assessment.

15. DATA BREACHES

15.1. All stakeholders are responsible for reporting known breaches internally to a senior manager or to the Data Protection Officer as soon as the breach is recognised. The responsible member of the senior leadership team should be informed.

15.2 The organisation will keep and implement a dedicated Data Breach Procedure to ensure any personal data breaches, including the facts relating to the data breach, its effects and the remedial action taken, are recorded in a data breach log and acted on accordingly.

15.3 The log shall be monitored and assessed by the Data Protection Officer. It will enable them to verify compliance with the data breach rules and raise awareness of minor breaches that may assist in identifying new data handling processes and training requirements.

15.4. In the case of a personal data breach resulting in a likely risk to the rights and freedoms of natural personals, and after consultation with the Data Protection Officer, the organisation shall, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Information Commissioner's Office.

15.5. Where the notification to the Information Commissioner's Office is not made within 72 hours, it shall be accompanied by reasons for the delay.

15.6 In order to evaluate the personal data breach, the organisation shall, without undue delay, immediately inform and involve the Data Protection Officer in the assessment of the breach and in the execution of the data breach procedure to contain and manage the breach.

15.7. **The notification to the Information Commissioner's Office shall at least:**

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

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

15.8 Where breaches are reportable to the Information Commissioner's Office, the senior leadership team should immediately inform members of the organisation's appropriate governance board or risk committee.

15.9 For examples of data breaches, please see Appendix 2.

16. SUBJECT ACCESS REQUESTS

16.1. The organisation is committed to:

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

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

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

16.3. **For information and guidance on how the organisation will deal with a Subject Access Request, see the Subject Access Request Procedure**

17. PUBLICATION OF INFORMATION

17.1. The organisation maintains and publishes a publication scheme on its website outlining classes of information that will be made routinely available, including policies and procedures.

17.2. Classes of information specified in the publication scheme will be made available quickly and easily on request.

17.3. The organisation will not publish any personal information, including photos, on its website without the permission of the affected individual.

17.4. When uploading information to the organisation's website, staff will be considerate of any metadata or deletions which could be accessed in documents and images on the site.

18. DBS DATA

18.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

18.2. Data provided by the DBS will never be duplicated.

18.3. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

18.4 Data Subjects have the right to appeal against any automated decision making, such as a DBS check

19. PHOTOGRAPHY IMAGES AND VIDEOS

19.1. Photographs and videos will only be collected and stored by the organisation, organisation staff and workforce with a documented lawful basis as in accordance with the organisation's Photography, Images and Video Policy document.

19.2. Photographs and videos will normally only be taken and used where they are deemed essential for performing the public task of the organisation or relative to providing education.

19.3. However, there may be occasions that arise where the organisation would like to celebrate the achievements of our pupils and therefore we may want to use images and videos of our pupils within promotional materials or for publication in the media, such as local, or even national, newspapers covering organisation events or achievements. If this is the case, we will seek the consent of the pupils, and their parents, where appropriate, before allowing the use of images or videos of pupils for such purposes.

19.4. Where photographs are required for other purposes, these purposes will be documented, and explicit consent will be sought.

19.5. The retention period for photographs and videos taken by the organisation, organisation staff and workforce will be documented in the organisation's retention policy. At the end of the retention period photographs will either be destroyed or they may be retained as photos for archiving purposes in the public interest.

19.6. Parents and others attending organisation events are allowed to take photographs and videos of those events for domestic purposes. For example, parents can take video recordings of an organisation's performance involving their child. The organisation does not prohibit this as a matter of policy.

19.7. The organisation does not, however, agree to any such photographs or videos being used for any other purpose but acknowledges that such matters are, for the most part, outside of the ability of the organisation to control or prevent.

19.8. The organisation asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

19.9. Whenever a pupil begins their attendance at the organisation, they, or their parent, where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose for which we do not have consent.

20. RETENTION POLICY

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

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

21.3. These checks will include the following questions being addressed:

- Have the documents been checked to ensure they are appropriate for destruction?
- Is retention required to fulfil statutory obligations or other regulatory obligations, including child protection?
- Is retention required for evidence?
- Is retention required to meet the operational needs of the service?
- Is retention required because the document or record is of historic interest, intrinsic value or required for organisational memory?

21.4 Retention data will be documented in the Record of Processing or taken as published in the IRMS school toolkit.

21. TRAINING

22.1. The organisation shall ensure that all members of staff receive data protection training, including training on information handling appropriate to their role, in order to ensure data protection competence in their role. This training shall be completed every two years as a minimum.

22. DATA PROCESSORS

23.1. The organisation contract with various organisations who provide services to the organisation, including:

- Payroll Providers – to enable us to pay our employees;
- Parent payment systems – to enable parents to pay for organisation meals, trips and/or uniforms;

- Pupil Assessment systems – to support us with the tracking and monitoring of pupil achievement;
- Communication systems – to enable us to effectively communicate with parents and pupils;
- organisation meal providers – to support with the provision and payment for organisation meals;
- Photographers – to enable us to store pupil photographs for safeguarding purposes;
- HR Systems – for the effective management of all aspects of staff management;

23.2. In order that these services can be provided effectively, we are required to transfer the personal data of data subjects to these data processors.

23.3. Personal data will only be transferred to a data processor if they agree to comply with our procedures and policies in relation to data security or if they put in place adequate measures themselves to the satisfaction of the organisation.

23.4. The organisation will always undertake due diligence of any data processor before transferring the personal data of data subjects to them.

23.5. Contracts with data processors will comply with Data Protection Legislation and contain explicit obligations on the data processor to ensure compliance with the Data Protection Legislation and compliance with the rights of Data Subjects.

23. CHANGES TO THIS POLICY

24.1 We may change this policy at any time. Where appropriate, we will notify data subject**s** of those changes.

This Policy was approved by the board of Governors on. It will be reviewed annually.

APPENDIX DEFINITIONS

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future;

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

Filing system means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by United Kingdom law, the controller or the specific criteria for its nomination may be provided for by United Kingdom law;

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with United Kingdom law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

Third party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Genetic data means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial

Data concerning health means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

Enterprise means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

Supervisory authority means in the UK the Information Commissioner's Office. In the case of data processed overseas in the European Union, this means an independent public authority which is established by a Member State pursuant to Article 51 of the GDPR;

Cross-border processing means either:

- processing of personal data which takes place in the context of the activities of establishments where the controller or processor is established in the UK and a third-party country; or

- processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the United Kingdom but which substantially affects or is likely to substantially affect data subjects in a third-party country;
- processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor outside the United Kingdom but which substantially affects or is likely to substantially affect data subjects in the United Kingdom;

Relevant and reasoned objection means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the United Kingdom;

Information society service means any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services;

International organisation means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;

Special categories of personal data means personal data:

- revealing racial or ethnic origin;
- revealing political opinions;
- revealing religious or philosophical beliefs or trade union membership;
- the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person;
- data concerning health or data concerning a natural person's sex life or sexual orientation;

Data breach: an incident or event in which personal and/or confidential data:

- has potentially been viewed or used by an individual unauthorised to do so;
- has had its integrity compromised;
- is lost or is unavailable for a significant period.

APPENDIX 2. EXAMPLES OF DATA BREACHES

- Loss or theft of paper records or loss or theft of equipment on which data is stored e.g. a laptop, mobile phone, tablet device or memory stick;
- A letter or email containing personal and/or confidential data sent to the wrong address (including internal staff or third parties) or an email to an unauthorised group of email boxes;
- Personal data disclosed orally in error in a meeting or over the phone – including "blogging" where information is obtained by deceiving The Organisation, or where information has been disclosed without confirming the true identity of the requester;
- Unauthorised access to information classified as personal or confidential e.g. attaching documents to an outlook diary appointment that is openly accessible;
- Posting information on the world wide web or on a computer otherwise accessible from the Internet without proper information security precautions;
- Sensitive information left on a photo-copier or on a desk in County Council premises;
- Unauthorised alteration or deletion of information;
- Not storing personal and confidential information securely;
- Not ensuring the proper transfer or destruction of files after closure of offices/buildings e.g. not following building decommissioning procedures;
- Failure to safeguard/remove personal data on office equipment (including computers and smart phones) before disposal/sale.

Examples of Breaches caused by IT Security Incidents:

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

APPENDIX 3. DEALING WITH SUBJECT ACCESS REQUESTS

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

If the information requested is for non-personal information i.e. is organisational or statistical information, this will fall under the FOIA or EIR, or BAU and will be dealt with, as follows: **All non-routine FOIA or EIR requests must be forwarded to the responsible member of staff (usually the Headteacher) and the Data Protection Officer within two working days of receipt of the request.**	**The FOIA and EIR stipulate that requests must be completed within 20 working days of the request – therefore the more swiftly request are being dealt with, the more likely The Organisation will meet its statutory deadlines.** **BAU requests need to be dealt with by an individual in that particular service area who can identify and locate the information requested and provide a response within a reasonable timeframe.**	**If the request is for non-routine/FOIA/EIR information contact the responsible member of staff (usually the Headteacher) and the Data Protection Officer.**
If the information requested is for the personal information of an individual for use in a criminal investigation by the police, or any other agency investigating criminal offences, this will fall under either the regulatory Investigative Powers Act 2000 (RIPA) or Data Protection Act 2018. **The request can be for either hard copy or any type of electronic information including email traffic ie the time and information that an email is sent.** **The request must be forwarded to the responsible member of staff (usually the Headteacher) and the Data Protection Officer within two days.**	**It is in the public interest that requests are identified and dealt with as quickly as possible.**	**Scan and email the request to the responsible member of staff (usually the Headteacher) and the Data Protection Officer as needed.**