Data Protection Policy

Applies to Prep, Pre-Prep and EYFS

Reviewed and approved:	Compliance Officer
	May 2024
Next review due:	May 2025

BARDWELL ROAD
OXFORD OX2 6SS
Tel: +44 (0)1865 315400
www.dragonschool.org

This policy must be read in conjunction with the Dragon School Privacy Notice.

In its everyday operations and in maintaining the Dragon Community, Dragon School makes use of a variety of data about identifiable individuals, including data about:

- Current, past and prospective governors, staff, supply staff, contractors, volunteers and anyone else working on behalf of the School
- Current, past and prospective pupils
- Parents of current, past and prospective pupils

In collecting and using this data, the School is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it. This legislation includes the UK General Data Protection Regulation and additional UK Data Protection law.

As part of Dragon School's commitment to safeguarding, the School has a particular duty to protect the personal data of its pupils.

The purpose of this policy is to set out the requirements of the relevant legislation and to describe the steps Dragon School takes to ensure that it complies with all relevant requirements.

This policy applies to all systems, people and processes that use or form part of the Dragon School's data processing, including governors, staff, supply staff, contractors and other third parties who have access to personal data held or collected by the School.

The following Dragon School policies and other documents should be read alongside this document:

- Privacy Notice
- Data Retention Policy
- Bring Your Own Device Policy
- Device and Network Security Policy
- Personal Use of The Dragon ICT Facilities Policy
- Security Policy (covering CCTV)
- Use of Cameras and Mobile Devices Policy
- Use of School-Issued Mobile Devices Policy

Where information regarding Data Protection Legislation in these or other school policies appears contradictory to this policy, the requirements set out in this policy will take precedence.

DATA PROTECTION LEGISLATION

The most significant pieces of Data Protection Legislation affecting the way in which Dragon School carries out its processing activities are set out below. Significant fines are applicable if any breach is deemed to occur under this legislation.

EU General Data Protection Regulation 2016 (EU GDPR) This is designed to protect the personal data of citizens of the European Union. This legislation will continue to be applicable from 1 January 2021 in relation to all data collected on or before 31 December 2020.

Data Protection Act 2018 This is the UK legislation under which the EU GDPR is applied in the UK.

UK General Data Protection Regulation (UK GDPR) This broadly mirrors the EU GDPR, however the UK has the independence to keep the framework under review.

It is the School's policy to ensure that our compliance with the relevance Data Protection Legislation is clear and demonstrable at all times.

DEFINITIONS IN DATA PROTECTION LEGISLATION

Personal data

'personal data' means:

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

The School will handle any personal data which can be linked in any way to an individual as described in this policy. This includes, but is not limited to, any personal data identifiable by way of a name, pupil code, staff code, national insurance number, or email address.

Processing

'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;

At Dragon School, processing should be interpreted as any action performed on personal data. Staff should consider the security and integrity of personal data at all times.

Controller

'controller' means:

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

The controller in relation to this policy is Dragon School.

PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA

There are a number of fundamental principles upon which the Data Protection Legislation is based.

These are as follows:

1. Personal data shall be:
    a. **processed lawfully, fairly and in a transparent manner** in relation to the data subject ('lawfulness, fairness and transparency');
    b. **collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
    c. **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed ('data minimisation');
    d. **accurate and, where necessary, kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
    e. **kept in a form which permits identification of data subjects for no longer than is necessary** for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the Data Protection Legislation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
    f. **processed in a manner that ensures appropriate security of the personal data**, including protection against unauthorised or unlawful processing and

against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The Controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

The School will ensure that it complies with all of these principles in its current processing activities and as part of the introduction of new methods of processing such as new IT systems.

RIGHTS OF THE INDIVIDUAL

The data subject (the person to whom the data relates) also has rights under the Data Protection Legislation. Further details are set out at "Appendix G – Rights of the Individual" below.

Each of these rights are supported by appropriate procedures within Dragon School that allow the required action to be taken within the timescales stated within the Data Protection Legislation.

Data Subject Request	**Timescale**
The right to be informed	When data is collected (if supplied by the data subject) or at the latest within one month (if not supplied by the data subject)
The right of access	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month
The right to object	On receipt of objection
Rights in relation to automated decision making and profiling.	Not specified

LAWFULNESS OF PROCESSING

There are six alternative ways in which the lawfulness of a specific case of processing of personal data may be established under the data protection legislation. It is the School's policy to identify the appropriate basis for processing and to document it, in accordance with the Data Protection Legislation. The options are described in brief in the following sections. The vast majority of processing at Dragon School does not require consent, however there are specific cases where consent is required.

Consent is sought for specific uses of images where those images are likely to be more privacy intrusive, for example where they are used by third party media. Consent will be sought from parents as appropriate. Uses of images which are solely internal do not routinely require consent. Clarification should always be sought from the Compliance Officer if in doubt.

Consent

Except where permissible under one of the other five bases for processing, Dragon School will always obtain specific consent from a data subject to collect and process their data. In the case of children, parental consent will be obtained on the child's behalf.

Transparent information about our usage of their personal data will be provided to data subjects at the time that consent is obtained and their rights with regard to their data explained, such as the right to withdraw consent. This information will be provided in a Privacy Notice, in an accessible form, written in clear language and free of charge.

If the personal data are not obtained directly from the data subject then the Privacy Notice will be provided to the data subject within a reasonable period after the data are obtained and at the latest within one month.

Performance of a Contract

Where the personal data collected and processed are required to fulfil a contract with the data subject, explicit consent is not required. This will be the case where the contract cannot be completed without the personal data in question.

Legal Obligation

If the personal data is required to be collected and processed in order to comply with the law, then explicit consent is not required.

Vital Interests of the Data Subject

In a case where the personal data are required to protect the vital interests of the data subject or of another natural person, then this may be used as the lawful basis of the processing. The School will retain reasonable, documented evidence that this is the case, whenever this reason is used as the lawful basis of the processing of personal data.

Task Carried Out in the Public Interest

Where the School needs to perform a task that it believes is in the public interest or as part of an official duty then the data subject's consent will not be requested. The assessment of the public interest or official duty will be documented and made available as evidence where required.

Legitimate Interests

If the processing of specific personal data is in the legitimate interests of the School and is judged not to affect the rights and freedoms of the data subject in a significant way, then this may be defined as the lawful reason for the processing. Individuals will however have the right to object to the processing of personal data.

PRIVACY BY DESIGN

The School has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect or process personal data will be subject to due consideration of privacy issues, including, where appropriate, the completion of one or more privacy impact assessments.

The privacy impact assessment will include:

- Consideration of how personal data will be processed and for what purposes.
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s).
- Assessment of the risks to individuals in processing the personal data.
- What controls are necessary to address the identified risks and demonstrate compliance with legislation.

Use of techniques such as data minimisation and pseudonymisation will be considered where applicable and appropriate.

CONTRACTS INVOLVING THE PROCESSING OF PERSONAL DATA

The School will ensure that all relationships it enters into that involve the processing of personal data are subject to a documented contract that includes the specific information and terms required by data protection legislation. This may be a contract provided to the School by the third party or a contract issued to the third party by the School. In all cases where personal data is to be processed on behalf of the School, a written agreement meeting the requirements of Data Protection Legislation and authorised by the Chief Operating Officer must be in place before processing takes place.

INTERNATIONAL TRANSFERS OF PERSONAL DATA

Transfers of personal data outside the UK will be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the UK GDPR. This depends on the UK's judgement as to the adequacy of the safeguards for personal data applicable in the receiving country and this may change over time. Where necessary appropriate contracts will be put into place with suppliers outside the UK.

At present, the UK has granted transitional adequacy decisions in relation to transferring data to all countries within the EEA, and all countries, territories, and international organisations covered by European Commission adequacy decisions as at 31 December 2020. These decisions may be reviewed over time.

DATA PROTECTION OFFICER

A defined role of Data Protection Officer (DPO) is required under the Data Protection Legislation if an organisation is a public authority, if it performs large scale monitoring or if it processes particularly sensitive types of data on a large scale. The DPO is required to have an

appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider.

Based on these criteria, Dragon School does not intend to appoint a Data Protection Officer.

DATA PROTECTION TEAM

The School's Compliance Officer is the primary lead on matters of Data Protection compliance. Additionally, the School has a Data Protection Team who work together to ensure compliance with Data Protection law. The team comprises of the:

- Chief Operating Officer
- Compliance Officer
- Director of ICT

In the absence of the Compliance Officer, other members of the Data Protection Team will deputise for this role. For serious Data Protection matters where it is appropriate to involve a member of the Senior Leadership Team, the Chief Operating Officer will be the primary lead.

The Data Protection Team can be contacted at the School address, on 01865 315400 or by email to data.protection@dragonschool.org.

BREACH NOTIFICATION

It is the School's policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with the Data Protection Legislation, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the Information Commissioner's Office will be informed as soon as practicable and in any event within 72 hours.

This will be managed in accordance with the Annex to this policy "Annex F - Dealing with Data Breaches", which sets out the overall process for handling data breaches.

CONSEQUENCES OF NON-COMPLIANCE

Under the Data Protection Legislation the Information Commissioner's Office has the authority to impose a range of fines of up to four percent of annual turnover or £17.5million, whichever is the higher, for infringements of the regulations.

ADDRESSING COMPLIANCE TO THE DATA PROTECTION LEGISLATION

The following actions are undertaken to ensure that the School complies at all times with the accountability principle of the Data Protection Legislation:

- The legal basis for processing personal data is clear and unambiguous.
- All personnel involved in handling personal data understand their responsibilities for following good Data Protection practice.
- Training in Data Protection has been provided to all staff.

- Rules regarding consent are followed.
- Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively.
- Regular reviews of procedures involving personal data are carried out.
- Privacy by design is adopted for all new or changed systems and processes.
- The following documentation of processing activities is recorded:
    - Organisation name and relevant details
    - Purposes of the personal data processing
    - Categories of individuals and personal data processed
    - Categories of personal data recipients
    - Agreements and mechanisms for transfers of personal data to non-EU countries including details of controls in place
    - Personal data retention schedules
    - Relevant technical and organisational controls in place

These actions are reviewed on a regular basis as part of the management process concerned with Data Protection.

ANNEX A – PROCESSING OF PERSONAL DATA WITHIN DRAGON SCHOOL

Personal data should always be processed with caution and with due regard to the rights and freedoms of the individual.

PERSONAL DATA WITHIN EMAILS

Personal data should not be distributed within email attachments. When personal data is recorded within an email body, this must be the minimum required and the email should not be forwarded to further recipients without first removing any personal data. Where possible, personal data should be shared as a link to a Box file or as reference to another existing system e.g. iSAMS.

Before sharing a file or a link, staff must always apply the minimisation principle:

- Reduce the amount of data shared to only that required to fulfil the specified task for which it is being shared
- Reduce the number of recipients to only those who are required to see the data for the specific task

Personal data to be shared should either be:

- Stored in an authorised IT system e.g. iSAMS
- Recorded in a file in an authorised file system e.g. Box

The text of emails should remain professional and factual at all times. Opinions should remain professional and as accurate as possible. Once recorded in an email these become personal data held by the School.

Large distribution lists should be avoided when sharing personal data. Emails containing personal data should be sent to a targeted list of recipients, including only those required for the task.

SECURING SHARED PERSONAL DATA

Wherever possible, the sharing of files containing personal data should be avoided. If the same data can be retrieved in a suitable format from an existing IT system (e.g. iSAMS), then reference to the material in iSAMS should be made rather than circulating data within a file or email.

If files containing personal data are to be shared, they should be stored on Box and a link to Box circulated. Box allows appropriate safeguards to be put in place including:

- Authorising only certain users of Box to view the file or folder
- Securing the link to the file or folder with a password
- Setting ‘expiry dates’ so that shared links will only remain active for a specified period of time.
- Restricting the file so it cannot be downloaded from Box
- Deletion of the original file allowing access to be removed

SHARING PERSONAL DATA WITH THIRD PARTIES

When sharing data with third parties outside Dragon School, the guidance in "Annex B – Transferring Personal Data to Third Parties" must be followed.

USE OF THIRD PARTY IT PROVIDERS (CLOUD STORAGE AND EMAIL SERVICES)

All communication by staff on behalf of the School must take place using a School email address. Only School issued devices should be used for electronic communication e.g. sending text messages on behalf of the School. Personal email addresses and cloud storage services not forming part of the School IT systems must not be used to transmit or store personal data except in an emergency.

PROCESSING DATA FOR NEW PURPOSES

All use of personal data must be documented and authorised by the Compliance Officer. Where an activity or process involves using data in a new way, this must be authorised in advance. e.g. exchanging data with a new activity provider, gathering data (including photos) through an event or activity.

Processing data in a new way requires an understanding of the basis on which such data is processed. It may require a new or supplementary Privacy Notice to be supplied to the individuals concerned and, where consent is required, this consent must be gathered in a compliant manner in advance of the data processing.

Clarification should always be sought from the Compliance Officer where the intended use of personal data is not already clearly established and documented in the School's Privacy Notices. Particular care should be taken when personal data about individuals outside the Dragon Community are involved as it is unlikely they will have been previously notified or have given consent in a compliant way.

ANNEX B - TRANSFERRING PERSONAL DATA TO THIRD PARTIES

Third parties who process data on behalf of the School are required to sign a written agreement before doing so. This may be in the form of a written agreement supplied by the third party, or in the form of a written agreement supplied by the School. In either case the agreement must ensure that personal data will be processed in accordance with the Data Protection Legislation and only in accordance with the School's specific instructions.

This agreement is essential for the School's compliance with Data Protection Legislation and will set out amongst other matters:

- who will be authorised to receive and process personal data.
- the method(s) of transfer to use when transferring personal data.
- the purpose(s) for which personal data will be used.
- the timeframe for which personal data will be held and the arrangements for return or destruction of the personal data after processing.
- confirmation that the third party will process personal data in line with the requirements of all Data Protection Legislation.

When transferring personal data to any external organisation or individual, the data must always be secured and/or encrypted. Where possible files should be shared using links to the Box system as this system allows appropriate access and retention control.

Information may be transferred into the systems of a third party, e.g. by completing a web form, however this must be performed in a secure manner. If there is any doubt, guidance should be sought from the Compliance Officer.

Routine sharing of information between the School and a child's parent does not require any additional agreement. However, due care should still be taken of any other reasons why data about a pupil may not be shared with a parent (e.g. legal restriction). Substantial requests for information, beyond routine School business, would become a Subject Access Request where additional rules then apply.

ANNEX C – ACCESS AND SECURITY CONTROLS FOR PERSONAL DATA

When accessing personal data, only the data necessary for a specific task should be viewed or retrieved. To enable this:

- School owned/managed IT systems have access controls set so that access is provided at the appropriate level to each member of staff.
    - Access controls are set by the IT Department and staff should request additional authorisation as required from the Director of ICT.
- Access controls for third party IT systems should be set appropriately. All third party IT systems should be installed/configured by, or with the assistance of, the Director of ICT.
    - The Director of ICT must retain the top level privilege for access control to all systems.

RELEASE OF PERSONAL DATA (EXTERNAL ENQUIRIES)

Establish the identity of the individual making the request

When any individual requests access to personal data e.g. an enquiry from a parent or relative, then the identity of the individual must always be established. This can be done informally e.g. in a face to face meeting with a familiar person, but must be done more formally when the person is unknown e.g. when receiving a telephone or email enquiry.

Personal data can only be released to:

- The data subject themselves (the personal data relating to a child belongs first and foremost to that child).
- In the case of a child, only an adult with parental responsibility for the child and even in such cases the parent does not have an absolute right to access the data.
    - Extended family members, family friends or others who do not have parental responsibility for the child should not be supplied with personal data relating to that child unless a clear instruction from a parent of that child has been received.

Advice should be sought if the request seems unusual or if the data being requested appears in any way to compromise the privacy of the individual.

TAKING PAPERWORK OFF SITE (E.G. AT HOME AND ON TRIPS)

Any paperwork removed from the School site must be the minimum required for a specified purpose. Paperwork must be stored securely and access limited appropriately. All paperwork should be returned to School once the specified purpose is complete for storage or to be destroyed.

In the case of trips, matches and other off site events, the organiser is responsible for ensuring all relevant paperwork containing personal data is returned and stored or destroyed as appropriate.

Misplaced or unaccounted for paperwork is a data breach which must be notified to the Compliance Officer.

USE OF PERSONAL IT EQUIPMENT

School IT systems are made accessible beyond the School site to enable staff to work and perform other duties while off site e.g. at home. This access is made available on the conditions that:

- School IT systems should only be accessed for specific, necessary purposes in the course of School business.
- All personal IT equipment (including equipment not owned by the School) used to access School IT systems must be encrypted and must be protected with a PIN, password or biometric access control.
- Where the personal IT equipment is shared, the account used to access school IT systems must not be made accessible to, or shared with, individuals who are not Dragon School staff (including limiting access by family members).
- Publicly accessible IT equipment or unsecured accounts should not be used to access school systems.
- Personal data must not be stored 'locally' i.e. on a PC, phone, tablet or other device not owned by the School or in a cloud service not managed by the School.
- Staff should take appropriate steps to further prevent unauthorised access to personal data e.g.
    - ensuring IT equipment is stored securely
    - clearing any 'cache' on the device regularly
    - installing appropriate anti-virus and anti-spyware tools

ANNEX D – DISPOSAL OF PERSONAL DATA

All personal data relating to an individual which no longer has a specific purpose must be disposed of securely. This means shredding of paper documents and full erasure of any electronic data including the contents of 'trash', the 'cache' and any backups.

Personal data should be retained no longer than is necessary for the purposes for which it was collected. In the case of paper copies of personal data (e.g. team lists) these should be retained no longer than is necessary for the purpose for which they were created.

Personal data should be retained in line with the School's Data Retention Policy. This sets out the principles and indicative retention times for the categories of personal data held by the School. While it is necessary to dispose of personal data in a timely fashion, the School has legal and other statutory duties to retain some personal data and records, so if in any doubt advice should be sought before disposing of documentation.

Where personal data is to be retained, this should exist as a single copy held either electronically or on paper in one of the School's 'official' filing systems e.g. the pupil files or staff files.

Personal data may be retained for a specific purpose; recent changes to Data Protection law do not mean all data must be erased. However, once personal data is no longer being used for its specified purpose it must be erased.

ANNEX E – DEALING WITH "SUBJECT ACCESS REQUESTS"

A subject access request is when an individual (the person to whom the data relates) requests details of the information held about them by Dragon School. Under the Data Protection Legislation, it is also called the 'Right of Access'.

An individual is entitled to:

- confirmation that their data is being processed.
- access to their personal data.
- The purposes of the processing.
- The categories of the personal data concerned.
- The recipients, or categories of recipients, of the data, if any, in particular any third countries or international organisations.
- The length of time that the personal data be stored for (or the criteria used to determine that period).
- The data subject's rights to rectification or erasure of their personal data and restriction of, or objection to, its processing.
- The data subject's right to lodge a complaint with a supervisory authority.
- Information about the source of the data, if not directly from the data subject.
- Whether the personal data will be subject to automated processing, including profiling and, if so, the logic and potential consequences involved.
- Where the data are transferred to a third country or international organisation, information about the safeguards that apply.

RECEIPT OF A SUBJECT ACCESS REQUEST

A subject access request can be made formally or informally. There is no set procedure required under the Data Protection Legislation and the data subject does not have to use the term "subject access request".

A subject access request can be made to any member of staff at the School and all members of staff must be aware of how to recognise one.

Any request to see the personal data we hold (other than that naturally disclosed during normal business) or to obtain further details about the processing we perform should be treated as a subject access request.

INTERNAL NOTIFICATION OF A SUBJECT ACCESS REQUEST

Any subject access request or any request which may be interpreted as such must be notified immediately by email to the Compliance Officer data.protection@dragonschool.org. The email should contain:

- The date the subject access request was made or received
- Details of the person who made the subject access request

- Details of the person about whom the subject access request was made if different (e.g. a pupil)
- Brief details of the nature of the request (if known)
- Contact details for the person who made the request

INTERNAL PROCESSING OF A SUBJECT ACCESS REQUEST

Following the initial notification, the Compliance Officer will take the lead in dealing with the subject access request. The member of staff receiving the request should not provide any personal data without first consulting the Compliance Officer.

Depending on the nature and complexity of the request, the Compliance Officer will put in place appropriate actions to retrieve and collate the information required.

The School will engage with external professionals, including legal advice, as necessary to ensure the request is processed in accordance with Data Protection law.

No other member of staff should take any further action in relation to a subject access request, including the disclosure of any information to the individual concerned, without the express authorisation of the Compliance Officer.

The following actions will be taken by the Compliance Officer:

1. Record the date and nature of the request and by/from whom it was received.
2. Assess the nature and extent of the initial request.
3. Contact the individual concerned to confirm details and identity, request any further information and confirm the expected date for completion of the request (normally one month from receipt).
4. Decide to action the request based on validity; request an amendment/clarification, charge a fee or refuse the request. Inform the individual of this decision without undue delay.
5. Request and receive any fee which may be applicable.
6. Direct appropriate personnel to retrieve the required personal data in line with established procedures.
7. Contact an external team (if required) who will then further process the request on the School's behalf.
8. If there is an undue delay in processing the request, or statutory time frames will not be met, inform the individual and agree the further course of action without undue delay.
9. Provide the requested information to the individual by a secure method.

TIMESCALES

In normal circumstances the School is required to fulfil subject access requests within one month of the initial request and at the earliest opportunity, without any undue delay. As such, all staff must cooperate fully and with urgency to all requests made in relation to a subject access request.

REQUIREMENTS SET OUT IN THE DATA PROTECTOIN LEGISLATION

The following general points are set out under the Data Protection Legislation:

1. Information shall be provided to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.
2. Information may be provided in writing, or electronically or by other means.
3. The data subject may request the information orally (e.g. over the telephone or face to face), as long as the identity of the data subject has been established.
4. We must act on a request from a data subject, unless we are unable to establish their identity.
5. We must provide information without undue delay and within a maximum of one month from the receipt of the request.
6. The response timescale may be extended by up to two further months for complex or a high volume of requests – the data subject must be informed of this within one month of the request, and the reasons for the delay given.
7. If a request is made via electronic form, the response should be via electronic means where possible, unless the data subject requests otherwise.
8. If it is decided that we will not comply with a request, we must inform the data subject without delay and at the latest within a month, stating the reason(s) and informing the data subject of their right to complain to the supervisory authority.
9. Generally, responses to requests will be made free of charge, unless they are "manifestly unfounded or excessive", in which case we will either charge a reasonable fee or refuse to action the request.
10. If there is doubt about a data subject's identity, we may request further information to establish it, however in normal circumstances, this will not affect the response timescale.

ANNEX F - DEALING WITH DATA BREACHES

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 (Article 4(12))

A data breach occurs when data is accidentally disclosed to a third party outside Dragon School or when data is taken by unauthorised means e.g. theft or hacking. A data breach can be something as simple as sending an email to the incorrect recipient, or can be a larger loss of personal data.

A data breach occurs when there is unauthorised access or accidental sharing of personal data internally e.g. if personal data is emailed to the wrong recipient within the School, emailed to too wide a distribution list, or accessed accidentally via our IT systems.

A data breach occurs when data is damaged, corrupted or lost such that the data cannot be retrieved when it would otherwise have been retained e.g. if a set of documents were accidentally shredded, lost, or a file accidentally deleted.

INTERNAL NOTIFICATION OF A DATA BREACH

All actual or suspected data breaches must be notified immediately by email to the Compliance Officer. This includes all internal and external breaches, of any severity. In addition, staff must take any immediate steps which may prevent a further impact of a breach e.g. requesting that an email be deleted without being read; securing a room or file if unauthorised access has been suspected.

The information which must be provided in the notification is:

- The date and time of the breach
- The nature of the data breach (what happened)
- The data contained within the breach (a summary description, not a copy of the data)
- The scale of the data breach (the volume of data and/or the number of individuals involved)
- Whether the data breach is likely to have a significant impact on the 'rights and freedoms' of the individual concerned (what is the likely impact or potential impact for the individual)
- What immediate steps have been taken in response (e.g. requesting deletion of an email; securing a room after suspected theft)

ACTIONS IN THE CASE OF A DATA BREACH

The Compliance Officer will take the lead in making appropriate notifications. These can include:

- Notifying the individual(s) concerned
- Notifying the Information Commissioner's Office

No other member of staff should contact the subject(s) of a data breach, or contact the ICO without first discussing the breach with the Compliance Officer.

The Compliance Officer will take the lead in any immediate and subsequent actions to reduce the impact of the breach and to prevent any further or recurring breaches from occurring.

The Compliance Officer will practice responses to potential breaches, including regular testing of IT procedures and security. External companies may be engaged to provide IT/security services to the School in the case of a breach to ensure all best practice measures are put in place in a timely manner.

RECORDING AND MONITORING

All data breaches, however small, must be recorded. The Compliance Officer will be responsible for maintaining the School's record of data breaches.

The causes and severity of data breaches will be reviewed by the Compliance Officer who will be responsible for advising on the appropriate measures required to prevent similar incidents recurring and for monitoring the implementation of those measures.

Records of data breaches will be reviewed periodically (not less than annually) by the Governing Body and Senior Leadership Team to ensure continued compliance and effective Data Protection procedures are in place.

ANNEX G – RIGHTS OF THE INDIVIDUAL

Data Protection Legislation provides individuals with a set of specific rights which the School must be prepared to respond to. These are set out below. All staff who process personal data must fully understand these rights.

Each of the rights has its own specific aspects and challenges for the School in complying with a request and doing so within the required timescales. In general, a proactive approach will be taken that places as much control over personal data in the hands of the data subject as possible, with a minimum amount of intervention or involvement required on the part of the School. This may be achieved by providing online access to the personal data so that the data subject can verify and amend it as required.

In some cases there is a decision-making process to be followed by the School regarding whether a request will be allowed or not. Where this is the case, the Compliance Officer will advise as to how the request should be fulfilled.

THE RIGHT TO BE INFORMED

At the point at which personal data are collected from the data subject or obtained from another source, there is a requirement to inform the data subject about our use of that data and their rights over it.

Where the data is obtained directly from the data subject (or in the case of a child, from the adult with parental responsibility) a copy of the School's applicable Privacy Notice must be provided at the point and time of data collection. This can be provided in physical copy, or as a link to the electronic document as published via the school website.

Where the School processes data which was not collected directly from the data subject, and the data subject has not previously been provided with the current Privacy Notice (or if there is any doubt), the Privacy Notice must be supplied as soon as possible and not later one month after collecting the data.

The School publishes a standard Privacy Notice covering all groups within the Dragon Community and a child friendly Privacy Notice for Children. Both a full Privacy Notice and the child friendly version must be supplied where the data relates to a child.

THE RIGHT OF ACCESS (SUBJECT ACCESS REQUEST)

A data subject has the right to ask the School whether we process data about them, to have access to that data and additional information as set out in "Annex E – Dealing with Subject Access Requests".

In most cases, the decision-making process for such requests will be straightforward unless it is judged that the request is manifestly unfounded or excessive. The compilation of the information is likely to require the input of several staff.

It is important that staff follow the separately documented procedure in "Annex E – Dealing with Subject Access Requests" in the case of a subject access request.

Any request exercised under this right should be referred immediately to the Compliance Officer.

THE RIGHT TO RECTIFICATION

Where personal data is inaccurate, the data subject has the right to request that it be corrected and incomplete personal data completed based on information they may provide.

Where necessary, the School will take steps to validate the information provided by the data subject to ensure that it is accurate before amending it.

Any request to rectify data must be communicated to all sections of the School which hold that personal data to ensure all records are maintained accurately.

THE RIGHT TO ERASURE

Also known as "the right to be forgotten", the data subject has the right to require the School to erase personal data about them without undue delay where one of the following applies:

- The personal data are no longer necessary for the purpose for which they were collected.
- The data subject withdraws consent and there is no other legal ground for processing.
- The data subject objects to the processing of the personal data.
- The personal data have been unlawfully processed.
- For compliance reasons, i.e. to meet the legal obligations of the School.
- Where the personal data was relevant to the data subject as a child.

Reasonable efforts should be made to ensure erasure where the personal data has been made public e.g. if the data features in a website or social media channel.

The School has a number of legal and statutory duties, including safeguarding, which require the School to retain information in line with the School's Data Retention Policy. The School will need to make a decision on each case of such requests as to whether the request can or should be declined for one of the following reasons:

- Right of freedom of expression and information
- Compliance with a legal obligation
- To protect archiving purposes in the public interest
- The personal data is relevant to a legal claim

Any request exercised under this right should be referred to the Compliance Officer.

THE RIGHT TO RESTRICT PROCESSING

The data subject can exercise the right to a restriction of processing of their personal data in one of the following circumstances:

- Where the data subject contests the accuracy of the data, until we have been able to verify its accuracy.
- As an alternative to erasure in the circumstances that the processing is unlawful.
- Where the data subject needs the data for legal claims but it is no longer required by us.
- Whilst a decision on an objection to processing is pending.

The School will need to make a decision on each case of such requests as to whether the request should be allowed. Any request exercised under this right should be referred to the Compliance Officer.

Where a restriction of processing is in place, the data may be stored but not further processed without the data subject's consent, unless for legal reasons (in which case the data subject must be informed). Other organisations who may process the data on our behalf must also be informed of the restriction.

THE RIGHT TO DATA PORTABILITY

The data subject has the right to request that their personal data be provided to them in a "structured, commonly-used and machine-readable format" and to transfer that data to another party e.g. to another school. This applies to personal data for which processing is based on the data subject's consent and the processing carried out by automated means, which in practice means that very little of the School's data will fall into this category.

Where feasible, the data subject can also request that the personal data be transferred directly from our systems to those of another provider.

THE RIGHT TO WITHDRAW CONSENT

The data subject has the right to withdraw consent where the basis for processing of their personal data is that of consent (i.e. the processing is not based on a different justification allowed by the Data Protection Legislation such as legitimate interest, contractual or legal obligation).

Dragon School has very few data processing activities which rely on consent (as defined in the Data Protection Legislation) as the basis for processing.

Before excluding the data subject's personal data from processing, it must be confirmed that consent is indeed the basis of the processing. If not, then the request may be rejected but otherwise, the request should be allowed.

In the case of a child, the giving or withdrawal of consent will be made by an adult with parental responsibility. However, we must also be mindful of the rights of the child over their

own data and so where a child raises objections to processing, this will be considered on a case-by-case basis.

Any request exercised under this right should be notified immediately to the Compliance Officer.

THE RIGHT TO OBJECT

The data subject has the right to object to processing that is based on the following legal justifications:

- For the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- For the purposes of the legitimate interests of the controller

Once an objection has been made, the School must justify the grounds on which the processing is based and suspend processing until this is done. Where the personal data is used for direct marketing we must no longer process the data.

Any request exercised under this right should be notified immediately to the Compliance Officer.

RIGHTS IN RELATION TO AUTOMATED DECISION MAKING AND PROFILING

The data subject has the right to not be the subject of automated decision-making where the decision has a significant effect on them, and can insist on human intervention where appropriate. The data subject also has the right to express their point of view and contest decisions.

There are exceptions to this right, which are if the decision:

- Is necessary for a contract
- Is authorised by law
- Is based on the data subject's explicit consent

In assessing these types of request, a judgement needs to be made about whether the above exceptions apply in the particular case in question.

Dragon School does not currently undertake any fully automated decision making, so in the context of Dragon School this request will not be relevant.

Any request exercised under this right should be referred to the Compliance Officer.

ANNEX H – TRAINING ARRANGEMENTS

Staff training is a key element of Data Protection compliance, ensuring all staff are aware of their obligations and the rights of individuals.

The School provides the following training to all members of staff (including where appropriate volunteers):

- Online Data Protection training – for all new staff as part of their induction
- Face to face training – for those unable to access the online provision or requiring additional support
- One-to-one support – for those where specific training or support needs have been identified

In addition, the School provides updates to all staff as required on changes to Data Protection law and refresher training regularly.

Where, as a result of evaluating a data breach or other Data Protection incident, staff training is required, the School will distribute appropriate information or provide additional training.

Members of the Data Protection Team undertake higher levels of Data Protection training to ensure they are adequately trained to carry out their duties.