RYDAL PENRHOS SCHOOL

Data Protection Policy

INTRODUCTION

This policy meets the requirements of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR. It also reflects the ICO's Code of Practice for the use of surveillance cameras and personal information.

The School processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller (as defined below). It is registered with the ICO, as is legally required.

It constitutes one of a suite of policies revolving around Information Technology matters, the other members of which are the following:

- E-Safety;
- Acceptable Use;
- Mobile 'Phone – Pupils;
- Mobile 'Phone – Staff;
- Mobile 'Phone – Parents & Visitors.

AIMS

Rydal Penrhos seeks to ensure that all personal data relating staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is held in paper or electronic format.

DATA PROTECTION PRINCIPLES

The GDPR is based on data protection principles with which the School must comply. The principles state that personal data must be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary to fulfil the purposes for which it is being processed;
- accurate and, where necessary, kept up-to-date;
- retained for no longer than is necessary for the purposes for which it is processed;
- processed in a way that ensures it is appropriately secure.

This policy sets out how the School aims to comply with these principles.

DEFINITIONS

Data controller:
This describes the person or organisation which determines the purposes and the means of the processing of personal data.

Data processor:
This denotes a person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

Data subject:
This concerns the identified or identifiable individual whose personal data is held or processed.

Personal data:
This pertains to any information relating to an identified, or identifiable, living individual; it may include the latter's name (including initials, identification number (in any context), location data, and online identifier (such as user name). It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Personal data breach:
This describes a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Processing:
This relates to anything which is done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Special categories of personal data:
This is defined as personal data which is more sensitive and therefore needs greater protection. It may include information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics (such as fingerprints, retina and iris patterns, where used for identification purposes), health (both physical or mental), and sex life or sexual orientation.

ROLES & RESPONSIBILITIES

This policy applies to all staff employed by the School, and also to external organisations or individuals working on the School's behalf. Staff who do not comply with this policy may face disciplinary action.

Governing Body:
They have overall responsibility for ensuring that Rydal Penrhos complies with all relevant data protection obligations.

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

Data Protection Officer:
The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring the School's compliance with data protection law, and developing related policies and guidelines where applicable.

He or she will provide an annual report of his or her activities directly to the Governing Body and, where relevant, will submits reports of his or her advice and recommendations on School data protection issues.

The DPO is also the first point of contact for individuals whose data is processed by the School, and for the ICO.
Full details of the DPO's responsibilities are set out in his or her job description.

The School's DPO is contactable via dpo@rydalpenrhos.com.

All staff:
All members of staff are responsible for the following:

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

COLLECTING PERSONAL DATA – LAWFULNESS, FAIRNESS & TRANSPARENCY

The School will only process personal data where it has one of the six 'lawful bases' (i.e. legal reasons) to do so under data protection law:

- the data needs to be processed so that the School can **fulfil a contract** with the individual, or the individual has asked the School to take specific steps before entering into a contract;
- the data needs to be processed so that the School can **comply with a legal obligation**;
- the data needs to be processed to ensure the **vital interests** of the individual or another person, i.e. to protect someone's life;
- the data needs to be processed so that the School, as a public authority, can **perform a task in the public interest or exercise its official authority**;
- the data needs to be processed for the **legitimate interests** of the School (where the processing is not for any tasks the School performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden;
- the individual (or his or her parent / carer, when appropriate in the case of a pupil) has freely given clear **consent.**

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

- the individual (or his or her parent / carer when appropriate in the case of a pupil) has given **explicit consent;**
- the data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**;
- the data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent;
- the data has already been made **manifestly public** by the individual;
- the data needs to be processed for the establishment, exercise or defence of **legal claims;**
- the data needs to be processed for reasons of **substantial public interest** as defined in legislation;
- the data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law ;
- the data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law ;
- the data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

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

- the individual (or his or her parent / carer when appropriate in the case of a pupil) has given **consent**;
- the data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent;
- the data has already been made **manifestly public** by the individual;
- the data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**;
- the data needs to be processed for reasons of **substantial public interest** as defined in legislation.

Whenever the School first collects personal data directly from individuals, it will provide them with the relevant information as required by data protection law.

The School will always consider the fairness of its data processing; it will ensure that it does not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects upon them.

COLLECTING PERSONAL DATA – LIMITATION, MINIMISATION & ACCURACY

Rydal Penrhos will only collect personal data for specified, explicit and legitimate reasons. The School will explain these reasons to the individuals when it first collects their data.

If the School wants to use personal data for reasons other than those given when it was first obtained, the School will inform the individuals concerned before this is done, and seek consent where necessary.

Staff must only process personal data when it is necessary in order to do their jobs.

The School will keep data accurate and, whenever necessary, up-to-date; inaccurate data will be rectified or erased when appropriate.

SHARING PERSONAL DATA

The School will not normally share personal data with anyone else without consent, but there are certain circumstances in which it may be required to do so. These include, but are not limited to, situations in which:

- there is an issue with a pupil or parent / carer that puts the safety of the School's staff at risk;
- the School need to liaise with other agencies – consent will be sought as necessary before doing this;
- the School's suppliers or contractors need data to enable them to provide services to the School's staff and pupils (for example, IT companies). When doing this, the School will:
    - only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law;
    - establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data that is shared;
    - only share data that the supplier or contractor needs to carry out their service.

Rydal Penrhos will also share personal data with law enforcement and government bodies where it is legally required to do so.

The School may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of its pupils or staff.

Whenever the School transfers personal data internationally, it will do so in accordance with data protection law.

SUBJECT ACCESS REQUESTS

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

- confirmation that their personal data is being processed;
- access to a copy of the data;
- the purposes of the data processing;
- the categories of personal data concerned;
- with whom the data has been, or will be, shared;
- for how long the data will be stored, or if this is not possible, the criteria used to determine this period;
- where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing;
- the right to lodge a complaint with the ICO or with another supervisory authority;
- the source of the data, if it has not been provided by the individual;
- whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual;
- the safeguards provided if the data is being transferred internationally.

Subject access requests can be submitted in any form, but the School may be able to respond to requests more quickly if they are made in writing and include the following details:

- the name of the individual;
- his or her address for correspondence;
- his or her contact number and email address;
- details of the information requested.

Should a member of staff receive a subject access request in any form, it must immediately be forwarded to the DPO.

CHILDREN & SUBJECT ACCESS REQUESTS

Personal data regarding a child belongs to that child, and not to the child's parents / carers. For a parent / carer to make a subject access request with respect to his or her child, the child must either be unable to understand his or her rights and the implications of a subject access request, or have given his or her consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights, as well as the implications of a subject access request. Therefore most subject access requests from parents or carers of pupils in Rydal Penrhos Prep School may be granted without the express permission of the pupil; however, this does not constitute a rule, and a pupil's ability to understand his or her rights will always be judged on a case-by-case basis.

Children aged 12 and above are generally thought to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents / carers of pupils in the Senior School may not be granted without the express permission of the pupil; once again, this does not constitute a rule, and a pupil's ability to understand his or her rights will always be judged on a case-by-case basis.

RESPONDING TO SUBJECT ACCESS REQUESTS

When responding to such requests, the School:

- may ask the person submitting the request to provide two forms of identification;
- may contact the person submitting the request by 'phone to confirm that the request has been made;
- will respond without delay and within one calendar month of receipt of the request (or receipt of the additional information needed to confirm identity, where appropriate);
- will provide the information free of charge;
- may tell the person submitting the request that the School will comply within three months of receipt of the request, where the request is complex or constitutes one of a set of requests. The school will inform the individual of this within one month, and will explain why the extension is necessary;

The School may not disclose information for a variety of reasons, such as if that information:

- might cause serious harm to the physical or mental health of the pupil or of another individual;
- would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests;
- would include another person's personal data that the School cannot reasonably anonymise, and the School does not hold the other person's consent, and it would be unreasonable to proceed without it;
- is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or examination scripts.

If the request is unfounded or excessive, the School may refuse to act on it, or may charge a reasonable fee to cover administrative costs. The school will take into account whether the request is repetitive in nature when making this decision.

Should Rydal Penrhos refuse a request, it will tell the individual why, and will advise him or her that he or she has the right to complain to the ICO, or he or she can seek to enforce his or her subject access right through the courts.

OTHER DATA PROTECTION RIGHTS OF THE INDIVIDUAL

In addition to the right to make a subject access request (see above) and to receive information when the School is collecting their data about how it is used and being processed, individuals also have the right to:

- withdraw their consent to processing at any time;
- ask the School to rectify, erase or restrict processing of their personal data (in certain circumstances);
- prevent the use of their personal data for direct marketing;
- object to processing which has been justified on the basis of public interest, official authority or legitimate interests;
- challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on his or her personal data with no human involvement);
- be notified of a data breach (in certain circumstances);
- make a complaint to the ICO;
- ask for their personal data to be transferred to a third party in a structured, commonly-used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO. Should staff receive such a request, they must immediately forward it to the DPO.

PARENTAL / CARER REQUESTS TO SEE THEIR CHILD'S EDUCATIONAL RECORD

In independent schools, parents, or those with parental responsibility do not have a legal right to free access to their child's educational record (which includes most of the information about a pupil) . However, Rydal School may agree to meet such a request, and a charge may be levied for this service. Any such request should be submitted to the Principal.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing examination marks before they are officially announced.

If the request is for a copy of the educational record, the School may charge a fee to cover the cost of supplying it ; this right applies as long as the pupil concerned is aged under 18.

BIOMETRIC RECOGNITION SYSTEMS

So as to improve the security of the campus, the School is planning to introduce biometric recognition systems. Wherever it uses pupils' biometric data as part of an automated biometric recognition system, it will comply with the requirements of the Protection of Freedoms Act 2012.

Parents / carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The School will obtain written consent from at least one parent or carer before it takes any biometric data from their child and processes that information.

Parents / carers and pupils have the right to choose not to use the School's biometric systems, and will be provided with an alternative method of authentication.

Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted in line with GDPR.

As required by law, if a pupil refuses to participate in, or to continue to participate in, the processing of his or her biometric data, the School will not process that data irrespective of any consent given by the pupil's parent / carer.

Where staff members or other adults use the school's biometric systems, Rydal Penrhos will also obtain their consent before they first take part in it, and will provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the School will delete any relevant data already captured.

CLOSED-CIRCUIT TELEVISION

The School is planning to introduce the use of Closed-Circuit Television (CCTV) in various locations around the School campus so as to ensure that it remains safe. The School will adhere to the ICO's Code of Practice for the use of CCTV; it does not need to ask individuals' permission to use CCTV, but it will make it clear whenever individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. Any enquiries about the CCTV system should be directed to the Estates Manager.

PHOTOGRAPHS & VIDEO

As part of Rydal Penrhos' activities, photographs may be taken and images recorded of individuals within the School.

The School will obtain written consent from parents / carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. The School will clearly explain how the photograph and / or video will be used to both the parent / carer and the pupil.

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

Whenever the School takes photographs and videos, their uses may include:

- posting on School noticeboards and in School magazines, brochures, newsletters, etc.;
- the use outside School by external agencies such as the School photographer, newspapers, campaigns etc.;
- online use on the School website or social media pages.

Consent can be refused or withdrawn at any time; if consent is withdrawn, Rydal Penrhos will delete the photograph or video and will not distribute it further.

When using photographs and videos in this way, the School will not accompany them with any other personal information about the child so as to ensure that the latter cannot be identified.

For further information about the School's use of photographs and videos, please refer to the Photography & Filming of Pupils Policy.

DATA PROTECTION BY DESIGN & DEFAULT

Rydal Penrhos will put measures in place to show that it has integrated data protection into all of its data processing activities, including:

- appointing a suitably qualified DPO, and ensuring that he or she has the necessary resources to fulfil his or her duties and to maintain his or her expert knowledge;
- only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law;
- completing data protection impact assessments where the School's processing of personal data presents a high risk to the rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process);
- integrating data protection into internal documents including this policy, any related policies and privacy notices;
- regularly training members of staff on data protection law, on this policy, on any related policies and on any other data protection matters. A record of attendance will be taken;
- regularly conducting reviews and audits to test the School's privacy measures to make sure that it is compliant;
- putting the appropriate safeguards in place if the School transfers any personal data outside the European Economic Area, where different data protection laws will apply;

- maintaining records of the School's processing activities, including:
    - for the benefit of data subjects, making available the name and contact details of the School and its DPO, and all the information the School is required to share about how it uses and processes their personal data (via its privacy notices);
    - for all personal data that the School holds, maintaining an internal record of the type of data, type of data subject, how and why it is using the data, any third-party recipients, any transfers outside the European Economic Area and the safeguards for those, retention periods and how it is keeping the data secure.

DATA SECURITY & STORAGE OF RECORDS

Rydal Penrhos will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- paper-based records and portable electronic devices such as laptops and hard drives that contain personal data are kept under lock and key when not in use;
- papers containing confidential personal data must not be left on office or classroom desks, in the Common Room, or left anywhere else where there is general access;
- passwords that are at least 8 characters long and contain letters and numbers are used to access School computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites;
- encryption software is used to protect all portable devices and removable media, such as laptops and USB devices;
- staff, pupils or Governors who store personal information on their personal devices are expected to follow the same security procedures as for School-owned equipment.

Whenever the School needs to share personal data with a third party, it will carry out due diligence and take reasonable steps to ensure that it is stored securely and adequately protected.

DISPOSAL OF RECORDS

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where the School cannot or does not need to rectify it or update it. For example, the School will shred or incinerate paper-based records, and will overwrite or delete electronic files; it may also use a third party safely to dispose of records on the School's behalf. If it does so, it will require the third party to provide sufficient guarantees that it complies with data protection law.

PERSONAL DATA BREACHES

The School will make every reasonable endeavour to ensure that no personal data breaches take place. However, in the unlikely event of a suspected data breach, it will follow the procedure as set out in Appendices 1 & 2.

When appropriate, the School will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:

- a non-anonymised dataset being published on the School website which shows the examination results of individual pupils;
- safeguarding information being made available to an unauthorised person;
- the theft of a School laptop containing non-encrypted personal data pertaining to pupils.

TRAINING

All staff and Governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, whenever changes to legislation, to guidance or to the School's processes make it necessary.

MONITORING ARRANGEMENTS

The DPO is responsible for monitoring and reviewing this policy.

This policy is subject to review on a biennial basis; however, it may require earlier revision in the light of any regulatory change which may come into force in the interim.

Last reviewed by LD / GCR:	February 2020
Approved by Governing Body:	February 2020
Next review:	February 2022

APPENDIX 1: PERSONAL DATA BREACH PROCEDURE

This procedure is based on the guidance on personal data breaches produced by the ICO, and operates as follows:

- on finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO;
- the DPO will investigate the report, and determine whether a breach has occurred. So as to reach this decision, the DPO will consider whether personal data has been accidentally or unlawfully:
    - lost;
    - stolen;
    - destroyed;
    - altered;
    - disclosed or made available where it should not have been;
    - made available to unauthorised people.
- the DPO will alert the Principal and the Chair of Governors;
- the DPO will make every reasonable effort to contain and to minimise the impact of the breach, assisted by relevant staff members or data processors where necessary (actions relevant to specific data types are set out at the end of this procedure);
- the DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen;
- the DPO will work out whether the breach must be reported to the ICO, and this must be judged on a case-by-case basis. If it is likely that there will be a risk to people's rights and freedoms, and any physical, material or non-material damage (e.g. emotional distress) may be caused, the DPO must notify the ICO. This risk may be caused as a result of the following:
    - loss of control over their data;
    - discrimination;
    - identify theft or fraud;
    - financial loss;
    - unauthorised reversal of pseudonymisation (for example, key-coding);
    - damage to reputation;
    - loss of confidentiality;
    - any other significant economic or social disadvantage to the individual(s) concerned.
- the DPO will document the decision (either way) in case it is challenged at a later date by the ICO or by an individual affected by the breach. Documented decisions will be stored within the secured DPO area on Office 365;
- whenever the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or by means of their 'breach report line' (0303 123 1113) within 72 hours. As required, the DPO will set out:
    - a description of the nature of the personal data breach including, where possible:
        - the categories and approximate number of individuals concerned;
        - the categories and approximate number of personal data records concerned.
    - the name and contact details of the DPO;
    - a description of the likely consequences of the personal data breach;
    - a description of the measures that have been, or will be taken, to deal with the breach and to mitigate any possible adverse effects on the individual(s) concerned.
- if all the above details are not yet known, the DPO will report as much as he or she can within 72 hours. The report will explain that there is a delay, the reasons for that delay, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible;

- the DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached, and any decision as to whether to contact individuals will be documented by the DPO. This notification will set out:
    - a description, in clear and plain language, of the nature of the personal data breach;
    - the name and contact details of the DPO;
    - a description of the likely consequences of the personal data breach;
    - a description of the measures that have been, or will be, taken to deal with the data breach and to mitigate any possible adverse effects on the individual(s) concerned.
- the DPO will notify any relevant third parties who can help mitigate the loss to individuals, for example, the police, insurers, banks or credit card companies;
- irrespective of whether it is reported to the ICO, the DPO will document each breach, and records will be held in the secured DPO area on Office 365.
- For each breach, this record will include the following details:
    - facts relating to the breach;
    - effects;
    - action taken to contain it and to ensure that it does not happen again (such as establishing more robust processes or providing further training for individuals).
- the DPO and Principal will meet to review what happened and how it can be prevented from happening again. This meeting will take place as soon as is reasonably possible

APPENDIX 2: ACTIONS TO MINIMISE THE IMPACT OF DATA BREACHES

Rydal Penrhos School will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. The School will review the effectiveness of these actions and amend them as necessary after any data breach.

Special category data (sensitive information, including safeguarding records):
Should such data be made available by email to unauthorised individuals, the following measures must be taken:

- the sender must attempt to recall the email as soon as he or she becomes aware of the error;
- members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error;
- if the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT Department to recall it;
- in any cases in which the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way;
- the DPO will ensure that the School receives a written response from all the individuals who received the data, confirming that they have complied with this request;
- the DPO will carry out an internet search to check that the information has not been made public. If it has, the School will contact the publisher / website owner or administrator to request that the information be removed from their website and deleted.