DATA PROTECTION POLICY

Date Agreed by the Governing Body	June 2018
Date to be reviewed	June 2019
Date of last review	June 2018
Governors Committee accountable for review	Personnel
Senior Leadership Team member accountable for review	ARW

1. Introduction

This is a policy for **Royal Grammar School, High Wycombe and** The Wycombe Royal Grammar School Foundation (hereinafter referred to as "**RGS High Wycombe**", "**we**", "**us**" or "**our**" as the context requires) and applies to an RGS High Wycombe employee, volunteer, Governor, Trustee, 'Friends of …' or PA member.

Data protection laws give people legal rights regarding how their personal data is processed. These rights apply to you, as well as to every individual whose personal data you process while working for us.

RGS High Wycombe has obligations under these data protection laws regarding how we treat the personal data we hold, what we do with it and who we share it with. We take these obligations seriously and we consider them as critical to our school and business.

2. What is this policy and why do you need to read it?

This policy sets out:

- details of our legal obligations in relation to personal data; and
- what your responsibilities are to ensure that we comply with them.

Everyone who works for us, whether as our employee or in another capacity as part of our school operations, must comply with this policy when processing personal data. In this policy references to "**you**" mean anyone that processes personal data for us, regardless of their employment status.

This policy applies whenever you handle personal data about anyone else, including pupils, parents, colleagues, job applicants and suppliers who are individuals or partnerships and Government Agencies, Child Protection Support Agencies.

You have a responsibility to read and comply with this policy and any other policies referred to in it, as well as to attend all mandatory data protection training that we provide to you. It is important that you understand what is required of you. Data protection is a serious matter and failure to comply with this policy may lead to disciplinary action up to and including dismissal.

Data protection legislation is enforced in the European Union by national or federal regulators (the "Regulator"). The respective Regulator can investigate complaints, audit our use of personal data and take action against us (and in some cases against you personally) for breach of this legislation. Enforcement action may include fines, criminal prosecution and preventing us from using personal data, which could prevent us from carrying on our business.

If we breach data protection legislation we could also have compensation claims made against us by individuals who are affected.

Our DPO and Deputy Headmaster will support us with data protection queries and they should be your first point of contact if you have any queries or concerns about this policy or about dealing with personal data.

3. Key terms used in this policy

"Personal data" is information (in any format) that relates to a living individual who can be identified from that information, either on its own or when it's combined with other information held by us.

- For example, names, addresses, contact details, salary details, job titles, CVs, CCTV images, credit card numbers, logon credentials, marketing preferences and data gathered from website cookies are all capable of being personal data.
- When considering whether data allows an individual to be identified you should think about it as a jigsaw piece and ask yourself whether if you were to put it together with all the other jigsaw pieces that we hold it would be possible to identify an individual.
- As you can see, the definition is broad, and increasingly – as technology enables us to identify individuals more easily – more data is likely to be regarded as personal data.

In this policy we refer to "processing" personal data. "Processing" means any activity carried out in relation to personal data, including collecting, recording, organising, storing, retrieving, altering, using, disclosing and destroying personal data.

"Data subject" is a term used in data protection legislation – it means the individual to whom the personal data relates. For simplicity, in this policy, we sometimes refer to these people as 'individuals'.

"Special personal data" (sometimes referred to as sensitive personal data or special category data) is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data (where it's processed to uniquely identify someone), data concerning health or someone's sex life or sexual orientation.

4. Data protection principles

There are six main principles, which we must follow in respect of all personal data we process. It is essential that you also comply with them when processing personal data for us.

The principles are that personal data must be:

- processed lawfully, fairly and in a transparent manner
- processed only for the specified, explicit and legitimate purpose(s) we collect it for
- adequate, relevant and limited to what we need in relation to the purpose(s) we collect it for
- kept accurate and kept up to date
- kept for no longer than necessary in relation to the purpose(s) we process it
- kept secure

We may be asked to demonstrate that we have complied with the data protection principles at any time. This data base is updated as required and, therefore, part of your role is to ensure that you make a record of any personal data that you process and how the processing complies with those principles in order that we can keep our records accurate and up to date.

5. Lawfulness, fairness and transparency

We must always have a "**lawful basis**" for processing personal data. The lawful bases which are most likely to be relevant to our processing are where:

- the individual has given his or her consent to the processing.
- the processing of the individual's personal data is **necessary to perform a contract** with that individual or to take steps at the request of the individual before entering into a contract.
- the processing is **necessary to comply with a legal obligation** to which we are subject.
- the processing is **necessary in order to protect the vital interests** of an individual.
- the processing is **necessary for the performance of a task carried out in the public interest** or in the exercise of official authority vested in us.
- the processing is **necessary for our legitimate interests**, provided those interests are not overridden by the individual's interests, rights or freedoms. RGS High Wycombe commits to carry out a balancing test between its legitimate interests and the individual's interests, rights or freedoms before collecting personal data on this specific lawful ground.

We must give individuals very specific information about how we process their personal data, to ensure that our processing is **fair and transparent**. This information is often referred to as a fair processing notice or privacy notice. We have set out below the procedures you should follow in respect of each channel by which we collect personal data:

- **Our websites and other digital platforms**. Our websites all include a permanently visible link to our online Privacy Policy and the relevant opt-ins. You should make sure that any new websites or digital platforms which you use or create contain the same links and opt-ins.

- **Privacy Notice**. Before any personal data is collected in relation to any RGS High Wycombe or third party system, function or application, the individual whose data we are collecting must be given certain specific information which is contained in our Privacy Notice. The Privacy Notice can be communicated in any number of methods provided it is easy for the recipient to access and read and that we can evidence receipt. The Privacy Notice can be obtained from the Deputy Headmaster and DPO whom you should consult for further guidance before completing and issuing the notices.

6. Special personal data –

An extra layer of rules apply when we process special personal data.

We still need to have a lawful basis for processing special personal data, but we also need an additional justification for processing it. The justifications that are most likely to be relevant are:

- Information crucial to the effective running of the schools as deemed by the Headmaster
- Safe Guarding/Child Protection concerns
- where the individual has given their explicit consent to the processing, or
- where the processing is necessary for employment or social security purposes.
- Medical information and care plans/ SEND information

If you have any questions or concerns in relation to processing special personal data and conducting Privacy Impact Assessments, you should contact our Deputy Headmaster and DPO.

A Privacy Impact Assessment is required in instances of high risk processing such as monitoring and surveillance of individuals and processing of sensitive personal data (other than minor instances ancillary to core processing activities). RGS High Wycombe's current and intended processing activities do not require a Privacy Impact Assessment to be carried out but, if this change and there is the potential to fall within scope, you will need to advise the Deputy Headmaster and DPO and a review will need to be undertaken.

7. Purposes for processing personal data

You should only process personal data that is necessary for a legitimate school or business purposes that is communicated to the individual and it mustn't be further processed for reasons which are not compatible with those purposes.

8. Adequate, relevant and necessary personal data

You should consider carefully how much personal data you actually need for the legitimate school or business purpose(s) you have identified for your processing activity. Do not collect personal data that is just "nice to have". It should only be the minimum necessary for the purpose.

9. Keeping personal data accurate

We must keep personal data accurate – and every reasonable step must be taken to erase or rectify inaccurate personal data. The best way to help us do this is to check with the individual that their personal data is correct at the time it is collected.

In order to ensure that personal data is kept up to date, you should ask the individual whether there have been any changes to their personal data each time you contact them.

You must update personal data with all necessary changes as soon as you become aware that it is inaccurate or out of date, and ensure that the updates are made across all relevant records and systems.

10. Retaining personal data

We can only keep personal data in a form which permits us to identify the individual concerned for as long as is necessary for the purpose(s) for which it has been collected. Even greater care needs to be taken to ensure that special personal data is not retained for longer than is necessary.

We must keep particular records for specific minimum and maximum periods by law. Otherwise we keep them for periods set out in our RGS Retention Policy. It is important that you comply with this for electronic and hard copy records.

The RGS Retention Policy can be accessed via Sharepoint.
If you have any questions about the RGS Retention Policy or you cannot identify the relevant period in the Record Retention Policy, please contact the Deputy Headmaster and DPO.

11. Security of personal data

We are required by law to have appropriate technical and organisational security measures in place to prevent unauthorised or unlawful processing and accidental loss or destruction of or damage to personal data. We may have to report any threat to or breach of security to the Information Commissioner's Office and to any affected data subjects.

We need everyone's help to keep personal data secure and everyone shares responsibility for this. You should help us do this by:

- complying with our E-Safety Policy, our acceptable use of ICT Policy, our Staff Code of Conduct, our Child Protection Policy, our RGS Retention Policy and following our GDPR staff guidance.
- considering carefully what format (e.g. paper or electronic) is required for the personal data you are processing;
- using common-sense, practical measures to protect the security of personal data (and in particular special personal data);
- before sending an email – pausing and checking that the content, attachments/enclosures and addresses/recipients are correct and that the email will be sent only to the people it's intended for;
- not sharing personal data with anybody (including people within our school) unless you are sure who they are and why they need access to the relevant personal data; and
- ensuring the ongoing confidentiality, integrity, availability and resilience of the systems processing systems and services we use for processing personal data.
  You must only use the personal data of others which you have access to in the performance of your role for our school and business purposes. You must not misuse it, for example by using the data for your own purposes, or those of family or friends, or disclosing it to others to use for their purposes. This would be a breach of our data security rules. It could be a breach of applicable data protection laws and indeed be a criminal offence in some cases.

12. Dealing with personal data breaches

What is a personal data breach and why is it important?

Dealing with personal data breaches is extremely important and they must be dealt with **immediately**.

A "**personal data breach**" is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Personal data breaches include the loss or theft of data or equipment on which data is stored (i.e. loss of memory stick or theft of an RGS High Wycombe laptop), inappropriate access controls allowing unauthorised use, human error (i.e. information sent to the incorrect recipient), hacking attacks and 'blagging' where information is obtained by deception. It also includes phishing attacks (where an attempt is made to obtain sensitive information such as usernames, passports and credit card details, often for malicious reasons).

RGS High Wycombe may have important legal reporting obligations with strict deadlines in relation to any actual, suspected or "near miss" incident. We have a legal obligation to notify the applicable Regulator of any security breach unless there is no risk whatsoever of individuals being affected. This must be done within 72 hours of becoming aware of the breach, and if we fail to notify, we could be at risk of severe

financial penalties. The clock starts from when the breach is discovered, not from when the breach is reported internally. We must also keep a register of all incidents.

We are relying on you to help us to comply with our legal obligations.

What should I do if I think there has been a personal data breach?

If you discover or suspect that there is or has been a security breach, you must inform our Deputy Headmaster and DPO. It is important that you do this immediately.

Even if the incident is an accident or you are at fault, it is essential that you do not hide it or cover it up. You must report any incidents or concerns straight away so we can try to minimise and control any damage, otherwise you may be at risk of stronger disciplinary action.

If you think there has been a potential personal data breach incident, you must understand the nature of the breach and in particular, what has happened to the data in question.

We'll need to know as much detail as possible in relation to the incident. For example:

- whether the data is lost or stolen;
- if so, whether there were any protections in place to prevent access or misuse;
- whether the data has been damaged or corrupted;
- if so, whether there were protections in place to lessen the impact of the loss.

We will need to know as much detail as possible as quickly as possible, to assess and make necessary decisions about what to do next. We will need to understand how serious the breach is, why it has happened, and whether it is ongoing so that we can stop it as soon as possible (and try to recover the data as quickly as possible).

We will also need your view on how many individuals' personal data has (or is likely to have) been affected by the breach, who those individuals are and how vulnerable the personal data is (e.g. what is the potential for misuse by a third party, does it include special personal data, whether there is any actual/potential harm that could come to any individuals, whether the incident is likely to lead to a substantial risk of individual harm, damage and/or distress etc.).

Once you have confirmed next steps with the Deputy Headmaster and DPO, you must work with them as they direct to take any actions required to deal with the breach. The Deputy Headmaster and DPO might need to inform the relevant Regulator and potentially any affected individuals.

You must always keep security breach incidents confidential and must not disclose them to anyone other than your immediate line manager and the Deputy Headmaster and DPO.

How can I help deal with the personal data breach?

The Deputy Headmaster and DPO will manage any personal data breach reported to them, which will involve the following steps:

- Fact-finding and containment of the incident: You must tell the Deputy Headmaster and DPO immediately. They will need to know what has happened, when it happened and how, what kind of data is involved e.g. special personal data, financial data etc. and how easily a data subject could be identified by that data, whether any systems or equipment have been affected, whether the personal data or device involved is protected (e.g. any encryption), how many individuals have or might have been affected (and who those individuals are), and who does or may now have access to the personal data and would they could potentially do with that data (i.e. what is the potential for harm to be caused to the individuals the personal data is about).

- Notification: The Deputy Headmaster and DPO will need to consider all of the information gathered in relation to the incident to determine whether they must report the incident to the data protection regulator and/or data subjects affected. Any notification to the data protection regulator must also include:

    - a description of 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;
    - the name and contact details of the DPO or other contact point where more information can be obtained;
    - a description of the likely consequences of the personal data breach; and
    - a description of the measures taken or proposed to be taken by RGS High Wycombe to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

- Lessons learned: To limit the chances or a similar incident happening again, we need to understand what went wrong and why and implement appropriate changes. You must cooperate and attend any training, and thoroughly read any revised guidance that we may issue from time to time.

If you have any security concerns or suggestions, please contact your line manager and the Deputy Headmaster and DPO.

13. Sharing personal data with other people

Third parties (i.e. agencies, companies, schools, businesses or people outside RGS, High Wycombe) may need to access the personal data we process, for example as part of providing services to us. However, we are only permitted to disclose personal data to third parties in certain limited circumstances.

When we are considering engaging a third party outside of RGS High Wycombe to process personal data on our behalf (a "third party service provider"), we must always have regard to the following:

- Due diligence - we must select a third party service provider who provides sufficient guarantees with respect to data security and the handling of personal data generally.
- Contractual obligations - we must ensure that there is a written contract in place with the third party service provider which includes specific data privacy obligations protecting personal data. Therefore, always check with the Deputy Headmaster and DPO before sharing any personal data with a third party service provider.
- Compliance monitoring - we must take reasonable steps to monitor the third party service provider's performance of the relevant security and processing obligations.

- International transfers - if engaging a third party service provider will or may involve personal data being processed abroad or overseas, in particular outside of the European Union, additional data protection and privacy considerations must be addressed and this generally means that additional clauses must be included in or as part of the contract with the third party.

We must never disclose personal data outside RGS High Wycombe to anyone other than a third party service provider except where this is lawful, including where it is necessary:

- to protect an individual's vital interests;
- to comply with a law, regulation or court order, for example, where requested by customs officials for the investigation of tax offences;
- to respond to any legitimate request for assistance by the police or other law enforcement agency;
- to engage and/or obtain advice from professional advisers (e.g. accountants, lawyers, external auditors etc.);
- to deal with any legal dispute or administrative claim between us and a third party (e.g. to that third party and lawyers representing them);
- to liaise with potential buyers or other third parties in connection with the disposal of or merging of any RGS High Wycombe asset(s)); or
- as otherwise permitted by, and in accordance with, applicable laws.

You should always check with our Deputy Headmaster and DPO if you are unsure whether or not you are permitted to disclose personal data to a third party.

14. Individuals' rights in relation to their personal data

Individuals have the following legal rights in relation to their personal data:

- Right to information

- Right of access – Individuals are entitled to receive confirmation from us as to whether or not we are processing personal data about them and, if we are, to access it and be provided with certain information in relation to it, such as the purpose(s) for which it is processed, the persons to whom it is disclosed and the period for which it will be stored;

- Right to rectification – Individuals can require us to correct any inaccuracies without undue delay;

- Right to erasure (also known as the right to be forgotten) – Individuals can require us to erase their personal data, without undue delay, if we no longer need it for the purpose for which we have it or if it is being unlawfully processed or if erasure is required to comply with a legal obligation to which we are subject. There are some exceptions to this right;

- Right to restriction of processing – Individuals can require us to restrict processing in certain circumstances including if the personal data is inaccurate or if the processing is unlawful;

- **Right to data portability** – Individuals can, in certain circumstances, receive the personal data in a structured, commonly used and machine-readable format so that it can be transferred to another provider; and

- **Right to object** – Individuals can object to:

  - any decision we make which is based solely on "automated processing" (i.e. without any human involvement) (**NB** There are some limits and exceptions to this right); and
  - us processing their personal data where we are relying on the lawful basis that our processing is necessary for a legitimate interest.

- **Right to withdraw consent** – Individuals have the right to withdraw their consent to our processing of their personal data at any time. If this happens, we must stop processing their personal data unless there is another lawful basis we can rely on – in which case, we must let the individual know. (**NB** If someone withdraws their consent, it won't impact any of our processing up to that point.)

15. Dealing with communications in relation to personal data

If you receive any communication from an individual or from any other person or body (including the Information Commissioner's Office) which suggests a breach has occurred or a breach may occur or an individual wishes to exercise data subject rights in relation to personal data, you must inform our Deputy Headmaster and DPO immediately, and provide details of the relevant communication.

We have to respond to certain requests from individuals in relation to their personal data within strict timescales, so it is very important that our Deputy Headmaster and DPO is made aware of each request **as quickly as possible**. You must also cooperate with our Deputy Headmaster and DPO by providing any other information and assistance that they may require.

Please do not, under any circumstances, respond to requests or communications about exercising rights in relation to personal data yourself without input from our Deputy Headmaster and DPO.

16. Personal data and direct marketing – Foundation, PA & 'Friends of….'

There are strict laws which govern direct marketing practices (in addition to data protection legislation). These are the e-privacy laws. This includes the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("**PECR**").

As you will note from the following, this is a complex area of law. **If you are not experienced in ensuring that our marketing is compliant with the law, please contact the Deputy Headmaster and DPO before undertaking any new marketing campaigns or methods.**

Amongst other things, PECR restricts unsolicited 'direct electronic marketing'. "Direct marketing" is defined as "the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals", and "electronic marketing" covers marketing by phone, fax, email, text or any other type of 'electronic mail' (there are different rules for live calls, automated calls, faxes, and electronic mail (which includes emails and text or SMS communications)).

RGS High Wycombe deals with parents, pupils, other schools and businesses. E-privacy laws currently mainly aim to protect consumers e.g. a.customer@gmail.com. Where e-mailing a corporate customer e.g. buyer.corp@buyercorp.com there is little concern. Where contacting your key contact at a corporate customer more care is needed e.g. mylead@buyercorp.com. This is because their business personal data is involved and some Regulators, in particular the ICO in the UK, would prefer us to treat these individuals like consumers. Our policy on this is to treat such individuals as consumers and this is reflected on all our websites and in our online Privacy Policy available here.

Under PECR, in order to undertake unsolicited direct electronic marketing to an individual (e.g. a consumer), you must either rely on:

- Consent (the default requirement), which must:
- be knowingly and freely given, clear, specific and unambiguous;
- be entity/brand specific and cover RGS High Wycombe and the type of communication it wants to use (e.g. email, text);
- involve some form of positive action – for example, ticking a box, clicking an icon, send an email or subscribing to a service – and the individual must fully understand that they are giving the organisation consent; and
- be evidenced.

Any group company or third party relying on the same consent must be named. Consent must be 'granular', so consent to such third party should be separated from the core consent (e.g. with another consent box). Consent to e-mail does not automatically cover texts. Pre-checked boxes and/or opt-outs are not encouraged and will be hard to justify as lawful. Any current consents that are not GDPR-compliant (i.e. do not meet the requirements) and that will be relied on will need to be refreshed.

(Legitimate interests under GDPR and) Soft opt-in under PECR – RGS High Wycombe must:

- have obtained the individual's contact details in the course of a sign-up sheet, meeting, sale (or negotiations for a sale) of a product or service to that individual (i.e. current parents and customers);
- only market its own similar products or services (and not for example another RGS High Wycombe 'group entities');
- give the individual a simple opportunity to refuse or opt out of the marketing, both when first collecting the details and in every message after that; and
- A soft opt-in can only be relied upon by the organisation that collected the contact details (i.e. just RGS High Wycombe, and not The Foundation/Friends of …?).

Soft opt in doesn't cover different goods/services or goods/services from third party/other group companies, or allow those other third parties to market to individuals.

You must not disguise or conceal RGS High Wycombe's identity in any marketing texts or emails, and you must provide a valid contact address for individuals to opt out or unsubscribe (which would mean consent was withdrawn). Unsubscribing should be very easy for customers and be possible electronically if consent was obtained electronically.

In any event, as a matter of good practice, you should:

- never buy or sell marketing lists from or to third parties; and
- always provide individuals with a simple means of unsubscribing from (or opting out of) our marketing communications, in every communication we send.

17. Training

RGS High Wycombe has and will continue from time to time to provide online training as necessary on data protection and other relevant topics related thereto.

It is your responsibility to take these training courses as soon as reasonably practical and devote the necessary time and attention required to complete the course and gain a full understanding of the topics covered. Any questions or concerns should be directed to the Deputy Headmaster and DPO.