Moon Hall School Reigate - Privacy Notice

Introduction

This notice is to help you understand how and why we collect personal information and what we do with that information. It also explains the decisions that you can make about your own information. It covers all data protection and related documents and policies at Moon Hall school, Reigate. It is for staff, pupils, parents, governors, FOMHSR, contractors, volunteers, alumni, and all other professional bodies and personnel associated with then school.

The school is registered with ICO and is also registered with the Charities Commission. The school is governed by Moon Hall Schools Educational Trust and is a Limited Company with charitable status.

For the purposes of the Data Protection Act (DPA) 1998 and in readiness for the new General Data Protection Regulations (GDPR), Moon Hall School Reigate, (MHSR), is the data controller of personal data about past, current and prospective pupils, their parents and guardians as well as data about past, current and prospective staff and third party contractors. This privacy notice sets out how MHSR uses and protects any information that you give us when you use this website. We are committed to ensuring that your privacy is protected. Should we ask you to provide certain information by which you can be identified when using this website, then you can be assured that it will only be used in accordance with this privacy statement. We may change this policy from time to time by updating this page. You should check this page from time to time to ensure that you are happy with any changes.

This information is provided in accordance with the rights of individuals under Data Protection Law to understand how their data is used. Staff, parents and pupils are encouraged to read this Privacy Notice and understand the School's obligations to its entire community. This Privacy notice can be found on the school website; www.moonhallschoolreigate.co.uk

Personal data processed by Moon Hall School Reigate collects and processes data about people to enable us to operate as a school. Information in both paper and digital formats is covered by the DPA. This includes:

- Objective or factual e.g. names, contact details, next-of-kin, birth dates, attendance records or

- Subjective, e.g. reports or grades, appraisals etc. that may include opinions

- **Sensitive**: the School may from time to time, process sensitive personal data such as medical conditions, ethnicity, religious beliefs, or criminal records and in relation to parents and/or guardians, financial information (**Article 9 GDPR**)

- Images: MHSR may publish images of staff and pupils engaging in School activities.

The first principle requires that you process all personal data lawfully, fairly and in a transparent manner. Processing is only lawful if you have a lawful basis under

Article 6 GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Your personal data will usually be collected directly from you, but some may be passed to the School by third parties (eg other schools)

This Privacy Notice also applies in addition to the School's other relevant terms and conditions and school policies including:

- School rules
- Any contract between the school and its staff or the parents of pupils
- The schools policy on taking, storing and using images of children
- The School's retention of records
- The School's safeguarding, pastoral and health & Safety policies
- The school's current and future IT policies, including 'Acceptable use'

Anyone who works for , or acts on behalf of the school (including staff, volunteers, governors, suppliers and service providers, should be aware of and comply with this Privacy Notice and the School's Data protection Policy.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Responsibility for Data Protection

The School has appointed Ken Hedley as the Chief Privacy Officer (CPO)

The appointment of a DPO will be confirmed

The CPO will deal with any requests and enquiries concerning the School's uses of your personal data (see section on Your Rights below) and endeavour to ensure that all personal data is processed in compliance with this policy and Data Protection Law.

Your Rights

Individuals have various rights under Data Protection Law to access and understand personal data about them held by the School, and in some cases ask for it to be erased or amended or for the School to stop processing it, but subject to certain exemptions and limitations.
Any individual wishing to access or amend their personal data, or wishing it to be transferred to another person or organisation, or who has some other objection to how their personal data is used, should put their request in writing to the CPO.

The School will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event within statutory time limits, which is one month in the case of requests for access to information. Consideration should also be given as to when you make the request as request during school holidays may experience delays.

The School will be better able to respond quickly to smaller, targeted requests for information. If the request is manifestly excessive or similar to previous requests, the School may ask you to reconsider or charge a proportionate fee, but only where Data Protection Law allows it.

You should be aware that certain data is exempt from the right of access. This may include information which identifies other individuals, or information which is subject to legal professional privilege. The School is also not required to disclose any pupil examination scripts (though examiners' comments may fall to be disclosed), nor any confidential reference given by the School for the purposes of the education, training or employment of any individual.

Pupil Requests

Pupils can make subject access requests for their own personal data, provided that, in the reasonable opinion of the School, they have sufficient maturity to understand the request they are making (see section Whose Rights below). Indeed, while a person with parental responsibility will generally be entitled to make a subject access request on behalf of younger pupils, the information in question is always considered to be the child's at law. A pupil of any age may ask a parent or other representative to make a subject access request on his/her behalf. Moreover (if of sufficient age) their consent or authority may need to be sought by the parent making such a request.

Pupils at Moon Hall Reigate aged 13 and above are generally assumed to have this level of maturity, although this will depend on both the child and the personal data requested, including any relevant circumstances at home. Slightly younger children may also sufficiently mature to have a say in this decision.

Parental requests

It should be clearly understood that the rules on subject access are not the sole basis on which information requests are handled. Parents may not have a statutory right to information, but they and others will often have a legitimate interest or expectation in receiving certain information about pupils without their consent. The school may consider there are lawful grounds for sharing with or without reference to that pupil. Parents will in general receive educational and pastoral updates about their children. Where parents are separated, the school will in most cases aim to provide the same information to each person with parental responsibility but may need to factor in all the circumstances including the express wishes of the child.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to
https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required

- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Why the school needs to process data.

In order to carry out its ordinary duties to staff, pupils and parents, the School may process a wide range of personal data about individuals (including current, past and prospective staff, pupils or parents) as part of its daily operation.

Some of this activity the School will need to carry out in order to fulfil its legal rights, duties or obligations, including those under a contract with its staff, or parents of its pupils.
Other uses of personal data will be made in accordance with the School's legitimate interests, or the legitimate interests of another, provided that these are not outweighed by the impact on individuals, and provided it does not involve special or sensitive types of data.

Purposes for which your data may be processed, your personal data (including sensitive personal data, where appropriate) is processed by the School strictly in accordance with the DPA in order to:

- support teaching and learning;
- monitor and report on pupils' progress;
- analyse and publish examination results and destinations of leavers;
- provide appropriate pastoral care including medical and other sensitive services;
- assess overall performance of the school;
- communicate to understand your needs and provide you with a better service
- collect information for central or national statutory authorities or exam boards;
- promote the school and its activities (e.g. events, performances, open days, reunions);

- assess and admit students;
- recruit and look after students and staff;
- monitor email communications or internet access to ensure compliance with School Rules, and strictly in accordance with the Terms and Conditions of the School's Contract for Responsible Use of IT;
- and for other reasonable purposes relating to its operation as a school and employer.

Unless parents request otherwise on the Data Collection Sheet completed for pupils joining the School, the School will not pass on information to any third party.

Third parties with whom the School may need to share personal data, MHSR does not share data with other organisations or individuals for commercial purposes. We may be required to share some data, including sensitive personal data, with third parties including local authorities, other public authorities, independent school bodies such as the Independent Schools Inspectorate (ISI) and the Independent Schools Council (ISC), health professionals, professional advisors, examination boards, travel organisations, school photographers and other service providers. Third parties who manage data on behalf of the school are known as data processors in respect of the personal data they receive, and must themselves comply with the DPA and the new GDPR.

Types of personal data processed by the school

This will include by way of example:

- Names, addresses, telephone numbers, e-mail addresses and other contact details;
- Car details (about those who use our car parking facilities);
- Bank details and other financial information, e.g. about parents who pay fees to the School;
- Past, present and prospective pupils' academic, disciplinary, admissions and attendance records (including information about any special needs), and examination scripts and marks;
- Where appropriate, information about individuals' health, and contact details for their next of kin;
- References given or received by the School about pupils, and information provided by previous educational establishments and/or other professionals or organisations working with pupils;
- Images of pupils (and occasionally other individuals) engaging in School activities (in accordance with the School's policy on taking, storing and using images of students).

How the school collects data

Generally, the School receives personal data from the individual directly (including, in the case of pupils, from their parents). This may be via a form, or simply in the ordinary course of interaction or communication (such as email or written assessments).

Who has access to personal data and who the school shares it with?

The School will need to share some personal information relating to its community with third parties, such as professional advisers (e.g. lawyers and accountants), therapists, relevant authorities (e.g. HMRC, police, medical agencies or the local authority) and commercial partners (e.g. caterers, travel and transport companies). For the most part, personal data collected by the School will remain within the School, and will be processed by appropriate individuals only in accordance with access protocols (i.e. on a 'need to know' basis).

Particularly strict rules of access apply in the context of:

- Medical records, held and accessed only by the School's Senior Management under the supervision of the School's senior first aider:
- Pastoral or safeguarding files;
- Financial information submitted under bursary applications.

However, a certain amount of any SEN pupil's relevant information will need to be provided to staff more widely in the context of providing the necessary care and education that the pupil requires. Staff, pupils and parents are reminded that the School is under duties imposed by law and statutory guidance (including Keeping Children Safe in Education; KCSIE September 2016) to record or report incidents and concerns that arise or are reported to it, in some cases regardless of whether they are proven, if they meet a certain threshold of seriousness in their nature or regularity. This may include file notes on personnel or safeguarding files, and in some cases referrals to relevant authorities such as the LADO or police. For further information about this, please view the School's Safeguarding Policy.

Finally, in accordance with Data Protection Law, some of the School's processing activity is carried out on its behalf by third parties, such as IT systems, web developers & Management Information Systems (Engage).

This is always subject to contractual assurances that personal data will be kept securely and only in accordance with the School's specific directions.

Security: We are committed to ensuring that your information is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect online.

How we use cookies: A cookie is a small file which asks permission to be placed on your computer's hard drive. Once you agree, the file is added and the cookie helps

analyse web traffic or lets you know when you visit a particular site. Cookies allow web applications to respond to you as an individual. The web application can tailor its operations to your needs, likes and dislikes by gathering and remembering information about your preferences. Overall, cookies help us provide you with a better website by enabling us to monitor which pages you find useful and which you do not. A cookie in no way gives us access to your computer or any information about you, other than the data you choose to share with us. You can choose to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. This may prevent you from taking full advantage of the website.

Links to other websites:

Our website may contain links to other websites of interest. However, once you have used these links to leave our site, you should note that we do not have any control over that other website. Therefore, we cannot be responsible for the protection and privacy of any information which you provide whilst visiting such sites and such sites are not governed by this privacy statement. You should exercise caution and look at the privacy statement applicable to the website in question.

We will not sell, distribute or lease your personal information to third parties unless we have your permission or are required by law to do so. You may request details of personal information which we hold about you under the Data Protection Act 1998. If you believe that any information we are holding on you is incorrect or incomplete, please write to or email us as soon as possible. We will promptly correct any information found to be incorrect.

How long we keep personal data

The School will retain personal data securely and only in line with how long it is necessary to keep for a legitimate and lawful reason. Typically, the legal recommendation for how long to keep ordinary staff and pupil personnel files is up to seven years following departure from the School.

However, incident reports and safeguarding files will need to be kept much longer, in accordance with specific legal requirements. If you have any specific queries about how this policy is applied, or wish to request that personal data that you no longer believe to be relevant is considered for erasure, please contact the CPO, whose contact details are below. (Ref. Retention Schedule)

However, please note that the School may have lawful and necessary reasons to hold on to some data. If the purpose for which the information was obtained has ceased and the personal information is no longer required, the data will be deleted or disposed of in a secure manner.

If anyone has any concerns or issues about how the retention data is applied or that anyone would request that any personal data should not be kept etc the data will be deleted and disposed of in a safe and secure manner.

MHSR have to comply with legal requirements and all procedures for data safety will be stored and locked away safely. They will be periodically reviewed.

The School's Retention of Records Guidelines gives details of the retention of different records; staff can access this on staff share, others can request a copy from the CPO.

The retention period guidelines have been taken from the 'Record Management Society of Great Britain; 'Retention guidelines for Schools'.

The lawful basis on which we use this information

Our lawful basis for collecting and processing pupil information information is defined under Article 6, and the following sub-paragraphs in the GDPR apply:

(a) Data subject gives consent for one or more specific purposes.

(c) Processing is necessary to comply with the legal obligations of the controller.

(d) Processing is necessary to protect the vital interests of the data subject.

(e) Processing is necessary for tasks in the public interest or exercise of authority vested in the controller(the provision of education).

Our lawful basis for collecting and processing pupil information information is also further defined under Article 9, in that some of the information we process is deemed to be sensitive, or special, information and the following sub-paragraphs in the GDPR apply:

(a) The data subject has given explicit consent.

(b) It is necessary to fulfil the obligations of controller or of data subject.

(c) It is necessary to protect the vital interests of the data subject.

(d) Processing is carried out by a foundation or not-for-profit organisation (includes religious, political or philosophical organisations and trade unions)

(g) Reasons of public interest in the area of public health

(i) It is in the public interest

A full breakdown of the information we collect on pupils can be requested from the school office.

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

An example of how we use the information you provide is:

The submission of the school census returns, including a set of named pupil records, is a statutory requirement on schools under Section 537A of the Education Act 1996.

Putting the school census on a statutory basis:

- *means that schools do not need to obtain parental or pupil consent to the provision of information*
- *ensures schools are protected from any legal challenge that they are breaching a duty of confidence to pupils*
- *helps to ensure that returns are completed by schools*

Requesting access to your personal data and your Data Protection Rights

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold, through a Subject Access Request.

Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.

Parents also have the right to make a subject access request with respect to any personal data the school holds about them.

If you make a subject access request, and if we do hold information about you or your child, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you or your child
- Tell you who it has been, or will be shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request please contact our CPO.

Complaints:

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our Chief Privacy Officer. Tel: 01306 611372

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Website disclaimer:

The information contained in this notice is for general information purposes only. The information is provided by MHSR and while we endeavour to keep the information up to date and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability with respect to the school website or the information, products, services, or related graphics contained on the school website for any purpose. Any reliance you place on such information is therefore strictly at your own risk. In no event will we be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or profits arising out of, or in connection with, the use of this website. Through this website you are able to link to other websites which are not under the control of the School. We have no control over the nature, content and availability of those sites. The inclusion of any links does not necessarily imply a recommendation or endorse the views expressed within them. Every effort is made to keep the website up and running smoothly. However, MHSR takes no responsibility for, and will not be liable for, the website being temporarily unavailable due to technical issues beyond our control.

Consent

Where the School is relying on consent as a means to process personal data, any person may withdraw this consent at any time (subject to similar age considerations as above). Please be aware however that the School may have another lawful reason to process the personal data in question even without your consent.

All individuals to positively opt-in on relying on consent.

That reason will usually have been asserted under this Privacy Notice, or may otherwise exist under some form of contract or agreement with the individual (e.g. an

employment or parent contract, or because a purchase of goods, services or membership of an organisation such as The PTA has been requested).

Sharing your information with others

Please be assured that we will not share your information for any other reason unless we are required by law or permitted to do so under this Privacy Notice. The main circumstances in which we will be permitted or required to disclose this is by law will be by court order, to government bodies and law enforcement agencies. However, sometimes we may share your information with third parties in the following ways:

- we may use carefully selected sub-processors to help us collect, store or manage your information. This will always be managed under the terms of a written data processing agreement;
- analytics and search engine providers that assist us in the improvement and optimisation of the Website.

Changes to this Privacy Notice

We may change this Privacy Notice at any time to ensure it always accurately reflects the way we collect, use and safeguard your Personal Information.

Please check this notice from time to time to ensure you are aware of any updates we may have made to our Personal Data handling practices. The date of the changes will be listed in the 'Last updated' section below First Version. We will endeavour to notify all of our current service users of any updates to this notice via email and we will post the relevant announcement on our website homepage.

We recommend that you print a copy of this page for your reference.

Transfer of data outside of the EU

We shall not transfer any personal data to any country outside of the European Economic Area unless we ensure that such personal data is subject to an adequate level of protection and appropriate legal safeguards in accordance with Data Protection Legislation.

Sharing your information with others

Please be assured that we will not share your information for any other reason unless we are required by law or permitted to do so under this Privacy Notice. The main circumstances in which we will be permitted or required to disclose this is by law will be by court order, to government bodies and law enforcement agencies. However, sometimes we may share your information with third parties in the following ways:

- we may use carefully selected sub-processors to help us collect, store or manage your information. This will always be managed under the terms of a written data processing agreement;
- analytics and search engine providers that assist us in the improvement and optimisation of the Website.

School Data Breach Procedure

This procedure has been produced based on current General Data Protection Regulations (GDPR) information. As further updates are released this procedure may be updated to reflect the changes.

Moon Hall School, Reigate holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by **Moon Hall School, Reigate** and all school staff, Governors, volunteers and contractors, referred to herein after as 'staff'.

Purpose

This breach procedure sets out the course of action to be followed by all staff at **Moon Hall School, Reigate** if a data protection breach takes place.

Article 33 of the General Data Protection Regulations
Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

   (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
   (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
   (c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

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

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article

Types of Breach

Data protection breaches could be caused by a number of factors. A number of examples are shown below:

- Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Poor data destruction procedures;
- Human Error;
- Cyber-attack;
- Hacking.

Managing a Data Breach

In the event that the School identifies or is notified of a personal data breach, the following steps should followed:

1. The person who discovers/receives a report of a breach must inform the Headmistress or, in their absence, either the Deputy Head Teacher and/or the School's Chief Privacy Officer (CPO). If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

2. The Headmistress/CPO (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT staff.

3. The Headmistress/CPO (or nominated representative) must inform the Chair of Governors as soon as possible. As a registered Data Controller, it is the school's responsibility to take the appropriate action and conduct any investigation.

4. The Headmistress/CPO (or nominated representative) must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the School's legal support should be obtained.

5. The Headmistress/CPO (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

a. Attempting to recover lost equipment.

b. Contacting the relevant authority, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned. Consideration should be given to a global email to all school staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual, making the enquiry, back. Whatever the outcome of the call, it should be reported immediately to the Headmistress/CPO (or nominated representative).

c. Contacting Surrey Council's Communications Division if part of the crisis service, so that they can be prepared to handle any press enquiries. The Council's Senior Communications Officer can be contacted by telephone on (01306) 885001

d. The use of back-ups to restore lost/damaged/stolen data.

e. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

f. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

Investigation

In most cases, the next stage would be for the Headmistress/CPO (or nominated representative) to fully investigate the breach. The Headmistress/CPO (or nominated representative) should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data;
- Its sensitivity;
- What protections were in place (e.g. encryption);

- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The Headmistress/CPO (or nominated representative) should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case by case basis.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the School is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the School's Complaints Procedure). The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach

Review and Evaluation

Once the initial aftermath of the breach is over, the Headmistress/CPO (or nominated representative) should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Senior Management Team and Full Governors meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources or Internal Audit for advice and guidance. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

Implementation

The Headmistress/CPO should ensure that staff are aware of the School's Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the School's Data Protection policy and associated procedures, they should discuss this with their line manager, CPO or the Headmistress.

Contact:

If you would like to discuss anything regarding this privacy notice, please contact the CPO at Moon hall School, Reigate on 01306 611372 or email:

emailenquiries@moonhallcollege.co.uk

First Version: May 2018

Last Updated: May 2018