Woodlands

respect resilience responsibility

General Data Protection Regulation (GDPR) Policy

Date: September 2018

Review Date: July 2019

1. GDPR – an introduction

This document sets out the school's responsibilities under the General Data Protection Regulation ("the GDPR") Act 2018 and provides guidance on the maintenance of and access to employment and educational records in accordance with the provisions of the Act.

The school has drawn on many resources in the creation of this new policy, most notably the two following documents:

- A "*Guide to the General Data Protection Regulation (GDPR)*" can be found on the Information Commissioner Office (ICO) website using the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711097/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

- The school also follows the "*Data protection: a toolkit for schools"* document published by the DfE. This document has been released as an open beta version, meaning that the document is a 'living document' which can be updated continually to accommodate relevant changes. At the time of writing this document is Version 1.0. This document can be accessed using the following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/740740/Data_Protection_Toolkit_for_Schools_OpenBeta_V1.0.pdf

1.1. What is the GDPR?

The GDPR is the new Data Protection legislation, introduced from May 25th 2018, superseding the Data Protection Act 1998. It imposes new rules on companies, government agencies, non-profits, and other organizations that offer goods and services to people in the EU, or that collect and analyse Data tied to EU residents. Even organisations outside EU need to be compliant, or otherwise face significant penalties.

The primary objective of the GDPR is to give citizens back control of their Personal Data. From an economic standpoint, the GDPR aims to simplify the regulatory environment for international business by unifying the regulation within the EU.

As the GDPR is a regulation and not a directive, it means that it is directly applicable in all EU member states from May 2018. A directive only directs member states to implement ruling, but does not enforce.

The GDPR applies to anyone or any organisation that processes, stores or is the subject of Personal Data.

1.2. Policy Statement and Objectives

Woodlands (the "school") is committed to the protection of all Personal and Sensitive Data for which it holds responsibility as the Data Controller and the handling of such Data in line with the 7 principles of GDPR, which are broadly similar to the eight principles that were previously identified in The Data Protection Act 1998. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/

Changes to Data Protection legislation shall be monitored and implemented in order to remain compliant with all requirements.

The objectives of this policy are to ensure that the school, its governors and employees are informed about, and comply with, their obligations under the GDPR and other associated Data Protection legislation.

Every person ("Data Subject") has rights with regard to how their personal information is handled. During the course of our activities we will "process" personal information about a number of different groups of people and we recognise that we need to treat it in an appropriate and lawful manner.

The type of information that we may be required to handle includes details of current, past and prospective employees, students, parents/carers and other members of students' families, job applicants, governors, volunteers, suppliers and other individuals that we communicate with. The information, which may be held on paper, on a

computer or other media, is subject to certain legal safeguards specified in the GDPR and other legislation. The GDPR imposes restrictions on how we may use that information.

This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy by members of staff will be taken seriously and may result in disciplinary action and in cases of serious breach, may result in dismissal.
Breach of the GDPR may expose the school to enforcement action by the Information Commissioner's Office (ICO), including the risk of fines. Furthermore, certain breaches of the Act can give rise to personal criminal liability for the school's employees.
At the very least, a breach of the GDPR could damage our reputation and have serious consequences for the school and for our stakeholders.

2. Status of the policy

This policy is discussed, evaluated, amended and ultimately approved at the first governing body meeting of each academic year. If it is at the pre-approval stage, there will be a "DRAFT" watermark on the document.
The policy sets out our rules on Data Protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

3. Data Protection Officer

The Data Protection Officer (the "DPO") is responsible for ensuring the school is compliant with the GDPR and with this policy. This post is held by the School Business Manager, Mrs Jenny Edwards and she can be contacted at:

Mrs Jenny Edwards
Woodlands Community College
Minstead Avenue
Harefield
Southampton
SO18 5FW
T – 02380 463303
E - jenny.edwards@woodlands.southampton.sch.uk

The DPO will play a major role in embedding essential aspects of the GDPR into the school's culture, from ensuring the Data Protection principles are respected to preserving Data Subject rights, recording Data Processing activities and ensuring the security of processing.

The DPO should be involved, in a timely manner, in all issues relating to the protection of Personal Data. To do this, the GDPR requires that DPO's are provided with the necessary support and resources to enable them to effectively carry out their tasks. Factors that should be considered include the following:

- senior management support;
- time for DPOs to fulfil their duties;
- adequate financial resources, infrastructure (premises, facilities and equipment) and staff where appropriate;
- official communication of the designation of the DPO to make known existence and function within the organisation;
- access to other services, such as HR, IT and security, who should provide support to the DPO;
- continuous training so that the DPO can stay up to date with regard to Data Protection developments;
- where a DPO team is deemed necessary, a clear infrastructure detailing roles and responsibilities of each team member;
- whether the school should give the DPO access to external legal advice in order for them to be advised of their responsibilities under this GDPR Policy.
- The DPO is responsible for ensuring that the school's processing operations adequately safeguard Personal Data, in line with legal requirements.

The school will ensure that the DPO does not receive instructions in respect of the carrying out of their tasks, which means that the DPO must not be instructed how to deal with a matter, such as how to investigate a complaint or what result should be achieved. Further, the DPO should report directly to the highest management level, i.e. the Governing Body.

The requirement that the DPO reports directly to the Governing Body ensures that the school's governors are made aware of the pertinent Data Protection issues. In the event that the school decides to take a certain course of action despite the DPO's advice to the contrary, the DPO should be given the opportunity to make their dissenting opinion clear to the Governing Body and to any other decision makers.

- A DPO appointed internally by the school is permitted to undertake other tasks and duties for the organisation, but these must not result in a conflict of interests with his or her role as DPO. It follows that any conflict of interests between the individual's role as DPO and other roles the individual may have within the organisation impinge on the DPO's ability to remain independent.
- In order to avoid conflicts the DPO cannot hold another position within the organisation that involves determining the purposes and means of processing Personal Data. Senior management positions such as Head Teacher and Bursar are likely to cause conflicts as are those that hold responsibility for safeguarding sensitive information, such as Child Protection Officer's (DSL's), SENDCO's and IT technical staff.
  Some other positions may involve determining the purposes and means of processing, which will rule them out as feasible roles for DPOs.
- In the light of this and in the event that the school decides to appoint an internal DPO, the school will take the following action in order to avoid conflicts of interests:
  - identify the positions incompatible with the function of DPO;
  - draw up internal rules to this effect in order to avoid conflicts of interests which may include, for example, allocating some of the DPO's other duties to other members of staff, appointing a deputy DPO and/or obtaining advice from an external advisor if appropriate;
  - include a more general explanation of conflicts of interests; and
  - include safeguards in the internal rules of the organisation and ensure that the job specification for the position of DPO or the service contract is sufficiently precise and detailed to avoid conflicts of interest.
- Any Data Subject who considers that the policy has not been applied appropriately in respect of Personal Data about yourself or others you should raise the matter with the DPO.

4. Definition of terms

- **Biometric Data** means Personal Data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images;
- **Consent** of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her;
- **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems or other media such as CCTV;
- **Data Subjects** for the purpose of this policy include all living individuals about whom we hold Personal Data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in relation to their Personal Data.
- **Data Controllers** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.
- **Data Users** include employees, volunteers, governors whose work involves using Personal Data. Data Users have a duty to protect the information they handle by following our Data Protection and security policies at all times;
- **Data Processors** means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller;
- **Parent** has the meaning given in the Education Act 1996 and includes any person having parental responsibility or care of a child;
- **Personal Data** means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by

reference to an identifier such as a name, an identification number, location Data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

- **Personal Data Breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;
- **Privacy by Design** means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR;
- **Processing** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- **Sensitive Personal Data/Special Category Data** means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic Data, Biometric Data for the purpose of uniquely identifying a natural person, Data concerning health or Data concerning a natural person's sex life or sexual orientation.

5. Data Protection Principles

The principles of the GDPR are broadly based upon those outlined in the Data Protection Act 1998.

The GDPR sets out seven key principles, which are broadly similar to the eight principles that were previously identified in The Data Protection Act 1998 and can be seen in the table below.

Data Protection Act 1998	The GDPR 2018
1st principle - Fairness: personal information must be processed fairly and lawfully. A key point is that the individual must have given his or her Consent to the information being processed.	Principle (a) – lawfulness, fairness and transparency. *Article 5(1) requires that Personal Data shall be* (a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
2nd principle - Purpose: personal information must only be used for the purposes for which it is obtained and no other	Principle (b) – purpose limitation *Article 5(1) requires that Personal Data shall be:* (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
3rd principle - Relevance: personal information must be adequate (enough to process it), relevant and not excessive (not asking for more than is needed)	Principle (c) – Data minimisation *Article 5(1) requires that Personal Data shall be:* (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('Data minimisation');
4th principle - Accuracy: personal information must be accurate and up to date	Principle (d) – accuracy *Article 5(1) requires that Personal Data shall be:* (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
5th principle - Preservation: personal information must only be held for as long as is necessary to complete the purpose for which it was obtained	Principle (e) – storage limitation *Article 5(1) requires that Personal Data shall be:* (e) kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed; Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
6th principle - Rights of the individual: personal information must only be used in accordance with the rights of the individual	Principle (f) – integrity and confidentiality *Article 5(1) requires that Personal Data shall be:* (f) processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."
7th principle - Security: we must take appropriate measures to: • Keep the personal information secure • Prevent unauthorised or unlawful use or access to it	Principle (g) – Accountability *Article 5(2) adds that:*

• Prevent damage or accidental loss	"The Controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."
8th principle - Transfer of Personal Data: we cannot transfer Personal Data to a country or territory outside of the European Economic Area (EEA) unless that country is able to demonstrate that an adequate level of protection exists for the processing of the Data.	

However there are a few key changes. Most obviously:

- Principle 6 (Rights of the individual) has been removed.
  This is now dealt with separately in Chapter III of the GDPR;
- Principle 8 (Transfer of Personal Data) has been removed.
  This is now dealt with separately in Chapter V of the GDPR;
- There is a new accountability principle (g).
  This specifically requires organisations to take responsibility for complying with the principles, and to have appropriate processes and records in place to demonstrate compliance.

In reference to the removal of Principle 6 (Rights of the individual), the GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to Data portability
- The right to object
- Rights in relation to automated decision making and profiling.

In reference to the removal of Principle 8 (Transfer of Personal Data), the GDPR provides the following rights for individuals:

- Personal Data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR.

5.1. Application of the Data Protection Principles at Woodlands

Principle (a) - Processed lawfully, fairly and in a transparent manner

The GDPR is intended not to prevent the processing of Personal Data, but to ensure that it is done fairly and without adversely affecting the rights of the Data Subject.
The Data Subject must be told who the Data Controller is (in this case the school), who the Data Controller's representative is (in this case the DPO), the purpose for which the Data is to be "Processed" by the school, and the identities of anyone to whom the Data may be disclosed or transferred.

For Personal Data to be processed lawfully, certain conditions have to be met. These may include:

- where the school have the Consent of the Data Subject; or where it is necessary for compliance with a legal obligation;
- where processing is necessary to protect the vital interests of the Data Subject or another person;
- where it is necessary for the performance of a task carried out in the Public Interest or in the exercise of official authority vested in the Controller.

Personal Data will only be processed for the specific purposes notified to the Data Subject when the Data was first collected, or for any other purposes specifically permitted by the Act. **This means that Personal Data must not be collected for one purpose and then used for another.**

If it becomes necessary to change the purpose for which the Data is processed, the Data Subject must be informed of the new purpose before any processing occurs.

Principle (b) – Purpose Limitation

Personal Data should only be collected to the extent that it is required for the specific purpose notified to the Data Subject, for example, in the Privacy Notice or at the point of collecting the Personal Data. Any Data which is not necessary for that purpose should not be collected in the first place.

- The school will be clear with Data Subjects about why their Personal Data is being collected and how it will be processed. The school cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless we inform the Data Subject of the new purposes and they have Consented where necessary.

Principle (c) – Data Minimisation

The GDPR states that Personal Data must be adequate, relevant and limited to what is necessary
The school will ensure that the Personal Data collected is adequate to enable us to perform our functions and that the information is relevant and limited to what is necessary.

In order to ensure compliance with this principle, the school will check all records at appropriate intervals for missing, irrelevant or seemingly excessive information and may contact Data Subjects to verify certain items of Data.

Employees must also give due consideration to any forms stakeholders are asked to complete and consider whether all the information is required. We may only collect Personal Data that is needed to operate as a school functions and we should not collect excessive Data.
The school will implement measures to ensure that Personal Data is processed on a 'Need to Know' basis. This means that the only members of staff or governors who need to know Personal Data about a Data Subject will be given access to it and no more information than is necessary for the relevant purpose will be shared.
In practice, this means that the school may adopt a layered approach in some circumstances, for example, members of staff or governors may be given access to basic information about a student or employee if they need to know it for a particular purpose but other information about a Data Subject may be restricted to certain members of staff who need to know it, for example, where the information is Sensitive Personal Data, (for example, child protection or safeguarding records) this would only be accessible to the schools' DSL's and the Head Teacher.

When Personal Data is no longer needed for specified purposes, it must be deleted/erased or anonymised in accordance with the school's Data Retention and Erasure Guidelines.

Principle (d) – Accuracy

The GDPR states that Personal Data must be accurate and, where necessary, kept up to date

The school will endeavour to ensure that all Personal Data that it collects is accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date Data should be destroyed in line with the school's Data Erasure Guidelines.

If a Data Subject informs the school of a change of circumstances their records will be updated as soon as is practicable.

Where a Data Subject challenges the accuracy of their Data, the school will immediately mark the record as potentially inaccurate, or 'challenged'. This practice is best achieved using the Sims Parent App, which will submit the Data directly to the school to import or decline.
In the case of any dispute, the school shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Data Protection Officer for their judgement. If the problem cannot be resolved at this stage, the Data Subject should refer their complaint to the Information Commissioner's Office. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.
A Data Subject continues to have rights under the GDPR and may refer a complaint to the Information Commissioner's Office regardless of whether the above procedure has been followed.

Principle (e) – storage limitation

The GDPR states that Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed. Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

The school is developing a records retention schedule and erasure guidelines to assist with this principle.

Principle (f) – integrity and confidentiality

All Personal Data must be processed in a manner that ensures appropriate security measures are in place.

The school has taken and is continuing to take steps to ensure that appropriate security measures are taken against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to it. Data Subjects may apply to the courts for compensation if they have suffered damage from such a loss.

The GDPR requires the school to put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

The school will develop, implement and maintain safeguards appropriate to our size, scope, our available resources, the amount of Personal Data that we control or maintain on behalf of others and identified risks (including use of passwords, permissions, secure locks, encryption and pseudonymisation where applicable).
The school will test the effectiveness of those safeguards at various intervals to evaluate and further improve security of our processing of Personal Data.

Data Users are responsible for protecting the Personal Data we hold. Data Users must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. Data Users must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

Data Users must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. Data Users must comply with all applicable aspects of our ICT Acceptable Use and E-Safety Policy and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data.

Maintaining Data security means guaranteeing the confidentiality, integrity and availability of the Personal Data, defined as follows:

- ***Confidentiality*** means that only people who are authorised to use the Data can access it.
- ***Integrity*** means that Personal Data should be accurate and suitable for the purpose for which it is processed.
- ***Availability*** means that authorised users should be able to access the Data if they need it for authorised purposes.

It is the responsibility of all members of staff and governors to work together to ensure that the Personal Data we hold is kept secure. We rely on our colleagues to identify and report any practices that do not meet these standards so that we can take steps to address any weaknesses in our systems. Anyone who has any comments or concerns about security should notify the Head Teacher or the DPO directly. The GDPRiS system, can also be used to report potential breaches of Data Protection.

Governors are likely to process Personal Data when they are performing their duties, for example, if they are dealing with employee issues, student exclusions or parent complaints.
Governors therefore need to be mindful of the information for which they hold as part of their school duties. This includes:

- Ensuring that Personal Data which comes into their possession as a result of their school duties is kept secure from third parties, including family members and friends.
- Ensuring they are provided with a copy of the school's ICT Acceptable Use and E-Safety Policy;
- Ensuring that any Personal Data sent to their electronic devices is secured appropriately (passwords, pin codes and erased once the Data has been used for its processing purpose);
- Taking appropriate measures to keep Personal Data secure, which includes ensuring that hard copy documents are securely locked away so that they cannot be access by third parties.
- Governors will be asked to read and sign an Acceptable Use Agreement.

Principle (g) – Accountability

The school must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with Data Protection Principles. The school is responsible for, and must be able to demonstrate, compliance with the Data Protection Principles.
The school must have adequate resources and controls in place to ensure and to document GDPR compliance including:

- appointing a suitably qualified DPO;
- implementing "Privacy by Design" when Processing Personal Data and completing Data Protection Impact Assessments (DPIAs) where Processing presents a high risk to rights and freedoms of Data Subjects;
- integrating Data Protection into internal documents including this GDPR Policy, related policies and Privacy Notices;
- providing appropriate training on the GDPR, this policy, related policies and Data Protection matters. The school must maintain a record of training attendance by school personnel. The school uses GDPRiS to record it's compliance with the GDPR.
- testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

6. Dealing with Subject Access Requests (SAR)

The GDPR extends to all Data Subjects a right of access to their own Personal Data.
The GDPR states that formal SAR's do not have to be made in writing, however the school has put into place systems to try to ensure that such requests are at least centrally recorded.

It is important that all members of staff are able to recognise that a written request made by a person for their own information is likely to be a valid Subject Access Request, even if the Data Subject does not specifically use this phrase in their request or refer to the GDPR.

In some cases, a Data Subject may mistakenly refer to the "Freedom of Information Act" but this should not prevent the school from responding to the request as being made under the GDPR, if appropriate.

Some requests may contain a combination of a Subject Access Request for Personal Data under the GDPR and a request for information under the Freedom of Information Act 2000 ("FOIA"). Requests for information under the FOIA must be dealt with promptly and in any event within 20 school days.

Any member of staff who receives a written request of this nature must immediately forward it to the DPO as the statutory time limit for responding is 30 days. Under the Data Protection Act 1998 (DPA 1998), Data Controllers previously had 40 calendar days to respond to a request.

As the time for responding to a request does not stop during the periods when the school is closed for the holidays, we will attempt to mitigate any impact this may have on the rights of Data Subjects to request access to their Data by implementing the following measures:

- all SAR's should be made electronically:
    - either via the school website: http://www.woodlands.southampton.sch.uk/about-us/gdpr/
    - or via email requests should be made directly by email to the DPO: data.protection@woodlands.southampton.sch.uk

The GDPR states that the school may no longer charge to the individual for provision of this information (previously a fee of £10 could be charged under the DPA 1998).

The school may ask the Data Subject for reasonable identification so that they can satisfy themselves about the person's identity before disclosing the information. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place.

A Parent would normally be expected to make a request on a child's behalf if the child is younger than 13 years of age.

Requests from parents in respect of their own child will be processed as requests made on behalf of the Data Subject (the child) where the student is aged under 13 (subject to any exemptions that apply under the Act or other legislation).

It should be noted that the Education (Pupil Information) (England) Regulations 2005 (the "Regulations") applies to maintained schools so the rights available to parents in those Regulations to access their child's educational records apply to the school. This means that following receipt of a request from a parent for a copy of their child's educational records, the school must provide a copy within 15 school days, subject to any exemptions or court orders which may apply. The school may charge a fee for providing a copy of the educational record, depending on the number of pages as set out in the Regulations. This is a separate statutory right that parents of children who attend maintained schools have so such requests should not be treated as a SAR.

Following receipt of a SAR, and provided that there is sufficient information to process the request, an entry should be made in the school's Subject Access Request log, showing the date of receipt, the Data Subject's name, the name and address of requester (if different), the type of Data required (e.g. Student Record, Personnel Record), and the planned date for supplying the information (not more than one calendar month from the request date). Should more information be required to establish either the identity of the Data Subject (or agent) or the type of Data requested, the date of entry in the log will be date on which sufficient information has been provided.

Where requests are "manifestly unfounded or excessive", in particular because they are repetitive, the school can:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse the request for information.

In a scenario where, the school refuses a request, the response must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month. Members of staff should refer to any guidance issued by the ICO on SARs and consult the DPO before refusing a request.

Certain information may be exempt from disclosure so members of staff will need to consider what exemptions (if any) apply and decide whether you can rely on them. For example, information about third parties may be exempt from disclosure. In practice, this means that you may be entitled to withhold some documents entirely or you may need to redact parts of them. Care should be taken to ensure that documents are redacted properly. Please seek further advice or support from the DPO if you are unsure which exemptions apply.

There is further information about exemptions to be added once the Data Protection Bill becomes law.

In the context of a school, a SAR is normally part of a broader complaint or concern from a Parent or may be connected to a disciplinary or grievance for an employee. Members of staff should therefore ensure that the broader context is taken into account when responding to a request and seek advice if required on managing the broader issue and the response to the request.

7. Sensitive Personal Data (Special Category Data)

Sensitive Personal Data, sometimes referred to as Special Category Data is Personal Data which the GDPR classifies as more sensitive, and so needs more protection.

In order to lawfully process Special Category Data, the school must identify both a lawful basis under Article 6 and a separate condition for processing Special Category Data under Article 9. These do not have to be linked.

There are ten conditions for processing Special Category Data in the GDPR itself, but the GDPR introduces additional conditions and safeguards.
You must determine your condition for processing Special Category Data before you begin this processing under the GDPR, and you should document it.

What's new?
Special Category Data is broadly similar to the concept of Sensitive Personal Data under the 1998 Act. The requirement to identify a specific condition for processing this type of Data is also very similar.

One change is that the GDPR includes genetic Data and some Biometric Data in the definition. Another is that it does not include Personal Data relating to criminal offences and convictions, as there are separate and specific safeguards for this type of Data in Article 10.

The conditions for processing Special Category Data under the GDPR in the UK are broadly similar to the Schedule 3 conditions under the 1998 Act for the processing of Sensitive Personal Data. More detailed guidance on the new special category conditions in the GDPR - and how they differ from existing Schedule 3 conditions - will be released by the ICO in due course.

The school must still have a lawful basis for your processing under Article 6, in exactly the same way as for any other Personal Data. The difference is that the school will also need to satisfy a specific condition under Article 9.

This is because Special Category Data is more sensitive, and so needs more protection. For example, information about an individual's race, ethnic origin, politics,

- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

In particular, this type of Data could create more significant risks to a person's fundamental rights and freedoms. For example by putting them at risk of unlawful discrimination.

The choice of lawful basis under Article 6 does not dictate which special category condition you must apply, and vice versa. For example, if you use Consent as your lawful basis, you are not restricted to using explicit Consent for special category processing under Article 9. You should choose whichever special category condition is the most appropriate in the circumstances – although in many cases there may well be an obvious link between the two. For example, if your lawful basis is vital interests, it is highly likely that the Article 9 condition for vital interests will also be appropriate.

What are the conditions for processing Special Category Data?
The conditions are listed in Article 9(2) of the GDPR:

7.1. Woodlands processing of Sensitive Personal Data

The school will be processing Sensitive Personal Data about our stakeholders. We recognise that the law states that this type of Data needs more protection. Therefore, Data Users must be more careful with the way in which we process Sensitive Personal Data.

When Sensitive Personal Data is being processed, as well as establishing a lawful basis (as outlined by principle (a) above), a separate condition for processing it must be met. In most cases the relevant conditions are likely to be that:

- the Data Subject's explicit Consent to the processing of such Data has been obtained
- processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, where we respect the essence of the right to Data Protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;
- processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving Consent;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Data Controller or of the Data Subject in the field of employment law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject.
- The school recognises that in addition to Sensitive Personal Data, we are also likely to Process information about our stakeholders which is confidential in nature, for example, information about family circumstances,

child protection or safeguarding issues. Appropriate safeguards must be implemented for such information, even if it does not meet the legal definition of Sensitive Personal Data.

Criminal convictions and offences

There are separate safeguards in the GDPR for Personal Data relating to criminal convictions and offences.

It is likely that the school will Process Data about criminal convictions or offences. This may be as a result of pre-vetting checks we are required to undertake on staff and governors or due to information which we may acquire during the course of their employment or appointment.

In addition, from time to time we may acquire information about criminal convictions or offences involving students or parents. This information is not routinely collected and is only likely to be processed by the school in specific circumstances, for example, if a child protection issue arises or if a parent/carer is involved in a criminal matter.

Where appropriate, such information may be shared with external agencies such as the child protection team at the Local Authority, the Local Authority Designated Officer and / or the Police. Such information will only be processed to the extent that it is lawful to do so and appropriate measures will be taken to keep the Data secure.

Sensitive SEN/CP Data

One of the most likely areas of Special Category Data that Woodlands holds is it's SEN and CP Data.
CP disclosures are made to the school via the Local Authority's secure Anycomms system.
Staff make disclosures using the CPOMS system. This provides appropriate access to relevant staff.
SEN information is stored in paper format, which should be locked away in filing cabinets in locked offices.
There is also SEN information stored on the school shared server, where appropriate permissions are assigned and on the SIMS database.

8. Processing in line with Data Subjects' rights

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

- withdraw Consent to Processing at any time;
- receive certain information about the Data Controller's Processing activities;
- request access to their Personal Data that we hold;
- prevent our use of their Personal Data for direct marketing purposes;
- ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate Data or to complete incomplete Data;
- restrict Processing in specific circumstances;
- challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
- request a copy of an agreement under which Personal Data is transferred outside of the EEA (European Economic Authority);
- object to decisions based solely on Automated Processing, including profiling (Automated Decision Making);
- prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
- be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- make a complaint to the supervisory authority (the ICO); and
- in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

The school is required to verify the identity of an individual requesting Data under any of the rights listed above. Members of staff should not allow third parties to persuade them into disclosing Personal Data without proper authorisation.

8.1. Providing information over the telephone

Any member of staff dealing with telephone enquiries should be careful about disclosing any Personal Data held by the school whilst also applying common sense to the particular circumstances. In particular they should:

- Check the caller's identity to make sure that information is only given to a person who is entitled to it.

- Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.
- Refer to the DPO for assistance in difficult situations. Staff should not feel pressurised into disclosing personal information.

9. Authorised disclosures

The school will only disclose Data about individuals if one of the lawful bases apply.

Only authorised and trained staff are allowed to make external disclosures of Personal Data. The school will regularly share Personal Data with third parties where it is lawful and appropriate to do so including, but not limited to, the following:

- Southampton City Council (HR and Safe Staffing Team)
- Hampshire County Council (Local Government Pension Scheme)
- the Department for Education
- the Disclosure and Barring Service - the Teaching Regulation Agency
- the Teachers' Pension Service
- Interserve Facilities Management
- Our external IT Broadband and Web Filtration Providers – Exponential-E & Lightspeed Systems
- Providers of educational IT systems – Google, Capita, PageOne, Groupcall, Impero, Lexia, Meritec, Micro Librarian Systems, Renaissance Learning, SISRA, Sumdog, Tucasi, MyMaths & SG World.
- HMRC
- the Police or other law enforcement agencies
- our legal advisors and other consultants
- insurance providers
- occupational health advisors
- Examination boards
- NHS health professionals including educational psychologists and school nurses
- Education Welfare Officers, Occupational Health advisers
- Courts, if ordered to do so
- Prevent teams in accordance with the Prevent Duty on schools
- other schools, for example when a student moves school or, if we are negotiating a managed move and we have Consent to share information in these circumstances
- confidential waste collection companies.

Some of the organisations we share Personal Data with may also be Data Controllers in their own right in which case we will be jointly Controllers of Personal Data and may be jointly liable in the event of any Data Breaches.

Data Sharing Agreements should be completed when setting up 'on-going' or 'routine' information sharing arrangements with third parties who are Data Controllers in their own right. However, they are not needed when information is shared in one-off circumstances but a record of the decision and the reasons for sharing information should be kept.

All Data Sharing Agreements must be signed off by the DPO who will keep a register of all Data Sharing Agreements.

The GDPR requires Data Controllers to have a written contract in place with Data Processors which must include specific clauses relating to the way in which the Data is Processed ("GDPR clauses"). A summary of the GDPR requirements for contracts with Data Processors is set out in Appendix 1.
It is the responsibility of the school to ensure that the GDPR clauses have been added to the contract with the Data Processor. The school should ensure that they are satisfied that the Data Processor is compliant with the GDPR and should only transfer Personal Data to a third-party Data Processor if they agree to put in place adequate technical, organisational and security measures themselves.
In some cases Data Processors may attempt to include additional wording when negotiating contracts which attempts to allocate some of the risk relating to compliance with the GDPR, including responsibility for any Personal Data Breaches, onto the school. In these circumstances, the member of staff dealing with the contract should contact the DPO for further advice before agreeing to include such wording in the contract.

10. Reporting a Personal Data Breach

The GDPR requires Data Controllers to notify any Personal Data Breach to the ICO and, in certain instances, the Data Subject.

A notifiable Personal Data Breach must be reported to the ICO without undue delay and where feasible within 72 hours, unless the Data Breach is unlikely to result in a risk to the individuals.

If the Breach is likely to result in high risk to affected Data Subjects, the GDPR, requires organisations to inform them without undue delay.

It is the responsibility of the DPO, or the nominated deputy, to decide whether to report a Personal Data Breach to the ICO.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

As the school is closed or has limited staff available during school holidays, there will be times when our ability to respond to a Personal Data Breach promptly and within the relevant timescales will be affected. We will consider any proportionate measures that we can implement to mitigate the impact this may have on Data Subjects when we develop our Security Incident Response Plan.

If a member of staff or governor knows or suspects that a Personal Data Breach has occurred, our Security Incident Response Plan must be followed. In particular, the DPO or such other person identified in our Security Incident Response Plan must be notified immediately. You should preserve all evidence relating to the potential Personal Data Breach.

11. Record keeping

The GDPR requires the school to keep full and accurate records of our Data Processing activities.

The school must keep and maintain accurate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

Records should include, at a minimum, the name and contact details of the Data Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place.

12. Training and audit

The school is required to ensure all school personnel have undergone adequate training to enable us to comply with Data privacy laws. Regular tests of our systems and processes should also be undertaken to assess compliance.

Members of staff must attend all mandatory Data Privacy related training.

13. Privacy By Design and Data Protection Impact Assessment (DPIA)

The school is required to implement "Privacy by Design" measures when Processing Personal Data by introducing appropriate technical and organisational measures (like extra layers of authentication, encryption and pseudonymisation) in an effective manner, to ensure compliance with Data Privacy Principles.

This means that we must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

- the state of the art
- the cost of implementation the nature, scope, context and purposes of Processing and

- the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

The school will conduct DPIAs and discuss the findings with the DPO in respect to high risk Processing, when implementing major system or business change programs involving the Processing of Personal Data including:

- use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes) Automated Processing including profiling and ADM
- large scale Processing of Sensitive Data and
- large scale, systematic monitoring of a publicly accessible area.

The school will also undertake a DPIA as a matter of good practice to help us to assess and mitigate the risks to Data Subjects. If our processing is likely to result in a high risk to the rights and freedom of children then a DPIA should be undertaken.

A DPIA must include:

- a description of the Processing, its purposes and the school's legitimate interests if appropriate;
- an assessment of the necessity and proportionality of the Processing in relation to its purpose;
- an assessment of the risk to individuals; and
- the risk mitigation measures in place and demonstration of compliance.

14. Policy Review

It is the responsibility of the Governing Body to facilitate the review of this policy on a regular basis, scheduled annually at the first governing body meeting of the academic year. Recommendations for any amendments should be reported to the DPO.

As stated in the introductory section, the guidance around GDPR is evolving and the school will therefore continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

The school will ensure that the DPO is aware of his or her obligations under this policy and that they receive the training and other support they need in order to fulfil this role.

15. Enquiries

Further information about the school's GDPR Policy is available from the DPO.

General information about the Act can be obtained from the Information Commissioner's Office: www.ico.gov.uk