DATA PROTECTION POLICY

Role responsible:	Assistant Principal, Data and Systems
Author:	Head of MIS
Approved by:	Corporation
Date Approved:	Approved by the Corporation: 14 December 2022 (Policy Review Group) Reviewed by the Corporation 13 July 2023 12 December 2024 **Revised and approved by Corporation 11 December 2025**
Next Review Date:	December 2026
Publication:	MS Teams
This policy reflects legislation at the time it was last reviewed. If there is a conflict between legislation and the policy, legislation will take precedence over anything printed in the policy	
Changes made:	• Name of DPO changed to 'Rob Davey' throughout • Changed the extension number of the DPO • 12.4.1 added clause re: MFA 'and possible multi-factor authentication where available' • Section 23 – there is no IT Security Policy. • Updated links in sections, 7.5 and 7.10
Version	2.1

CONTENTS

1. OVERVIEW

Wyke Sixth Form College's reputation and future growth are dependent on the way the College manages and protects Personal Data. Protecting the confidentiality and integrity of Personal Data is a key responsibility of everyone within the College.

As an organisation that collects, uses and stores Personal Data about its employees, students, suppliers (sole traders, partnerships or individuals within companies), Corporation Members, parents and visitors, the College recognises that having controls around the collection, use, retention and destruction of Personal Data is important in order to comply with the College's obligations under Data Protection Laws and in particular its obligations under Article 5 of GDPR.

The College has implemented this Data Protection Policy to ensure all College personnel are aware of what they must do to ensure the correct and lawful treatment of Personal Data. This will maintain confidence in the College and will provide for a successful working and learning environment for all.

College personnel will receive a copy of this Policy when they start and may receive periodic revisions of the Policy. The Policy does not form part of any member of the College personnel's contract of employment and the College reserves the right to change this Policy at any time. All members of college personnel are obliged to comply with this Policy at all times. Any failure to follow the policy can therefore result in disciplinary proceedings as outlined in the Disciplinary Policy.

Any member of staff who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the designated Data Protection Officer initially. If the matter is not resolved it should be raised as a formal grievance.

If you have any queries concerning this Policy, please contact our Data Protection Officer, who is responsible for ensuring the College's compliance with this Policy.

2. ABOUT THIS POLICY

2.1 This Policy (and the other policies and documents referred to in it) sets out the basis on which the College will collect and use Personal Data either where the College collects it from individuals itself, or where it is provided to the College by third parties. It also sets out rules on how the College handles uses, transfers and stores Personal Data.

2.2 It applies to all Personal Data stored electronically, in paper form, or otherwise.

3. DEFINITIONS

Children's Code	Also known as the Age-Appropriate Design Code (Children's Code/AADC) is a data protection code of practice for online services, such as apps, online games, and web and social media sites, likely to be accessed by children. The College will aim to abide by the code where relevant.
College	Wyke Sixth Form College

College Personnel	Any College employee, worker or contractor who accesses any of the College's Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the College.
Controller	Any entity (e.g. company, organisation or person) that makes its own decisions about how it is going to collect and use Personal Data. A Controller is responsible for compliance with Data Protection Laws. Examples of Personal Data the College is the Controller of include employee details or information the College collects relating to students. The College will be viewed as a Controller of Personal Data if it decides what Personal Data the College is going to collect and how it will use it. A common misconception is that individuals within organisations are the Controllers. This is not the case - it is the organisation itself which is the Controller.
Data Protection Laws	The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.
Data Protection Officer	Our Data Protection Officer is Rob Davey, and can be contacted at: dpo@wyke.ac.uk
EEA	Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden.
ICO	The Information Commissioner's Office, the UK's data protection regulator.
Individuals	Living individuals who can be identified, *directly or indirectly*, from information that the College has. For example, an individual could be identified directly by name, or indirectly by gender, job role and office location if you can use this information to work out who they are. Individuals include employees, students, parents, visitors and potential students. Individuals also include partnerships and sole traders.
Personal Data	Any information about an Individual (see definition above) which identifies them or allows them to be identified in conjunction with other information that is held. It includes information of this type, even if used in a business context. Personal data is defined broadly and covers things such as name, address, email address (including in a business context, email addresses of Individuals in companies such as firstname.surname@organisation.com), IP address and also more sensitive types of data such as trade union membership, genetic data and religious beliefs. These more sensitive types of data are called "Special Categories of Personal Data" and are defined below. Special Categories of Personal Data are given extra protection by Data Protection Laws.
Processor	Any entity (e.g. company, organisation or person) which accesses or uses Personal Data on the instruction of a Controller. A Processor is a third party that processes Personal Data on behalf of a

	Controller. This is usually because of the outsourcing of a service by the Controller or the provision of services by the Processor which involve access to or use of Personal Data. Examples include: where software support for a system, which contains Personal Data, is provided by someone outside the business; cloud arrangements; and mail fulfilment services.
Special Categories of Personal Data	Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.

4. COLLEGE PERSONNEL'S GENERAL OBLIGATIONS

4.1 All College Personnel must comply with this policy. Everyone who works for, or with, the college has some responsibility for ensuring data is collected, stored and handled appropriately and in accordance with GDPR.

4.2 College Personnel must not release or disclose any Personal Data:

4.2.1 outside the College; or

4.2.2 inside the college to College Personnel not authorised to access the Personal Data; or

4.2.3 without specific authorisation from their manager or the Data Protection Officer; this includes by phone call or in emails.

4.3 College Personnel must take all steps to ensure there is no unauthorised access to Personal Data whether by other College Personnel who are not authorised to see such Personal Data or by people outside the College. Personnel should keep all data secure, including taking sensible precautions and following the guidelines below:

4.3.1 Strong passwords must be used for any internal or external systems that use personal data, and these passwords should never be shared.

4.3.2 College data should not be disclosed to unauthorised people, either within the College or externally.

4.3.3 Employees should request help from their line manager or the Data Protection Officer if they are unsure about any aspect of data protection.

4.4 In addition to the responsibilities above relating to all Personnel, the following people have key areas of responsibility:

4.4.1 The Corporation is ultimately responsible for ensuring that Wyke Sixth Form College meets its legal obligations in relation to the GDPR.

4.4.2 The Senior Management Team is responsible for management of the Data Protection risk within college, and in providing leadership for consistent college-wide adoption of policies and procedures associated with it.

4.4.3 All College managers are responsible for:

- ensuring they are satisfied with the legality of holding and using the information collected by staff in their area;
- ensuring that the use of personal data complies with all appropriate College policies
- ensuring that relevant staff they manage undertake the GDPR training;
- referring any non-routine requests for disclosure, requests for subject access and requests to cease processing to the Data Protection Officer;
- raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay;
- checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing.

4.4.4 The Data Protection Officer is responsible for:

- Keeping Corporation updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data that the college holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the College's sensitive data.
- Maintaining the College ICO Data Protection registration.
- Make recommendations to the College Leadership Team (CLT) regarding Data Protection/GDPR Policy and good practice.

4.4.5 The Head of IT is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the college is considering using to store or process data. For instance, cloud computing services.

4.5 Further details of GDPR responsibilities of the Data Protection Officer and the Head of IT can be found in Appendices 1 and 2 respectively.

4.6 The College will provide regular training to all employees to help them understand their responsibilities when handling data.

5. STUDENT OBLIGATIONS

5.1 Students must ensure that all personal data provided to the college are accurate and up to date. They must ensure that changes of address, mobile phone, email address, emergency contact details etc. are notified to the Office, MIS or Tutor as soon as is possible.

5.2 Students must not seek to gain unauthorised access to personal information.

5.3 Students must comply with all College policies regarding the use of IT facilities, including the IT and Internet Acceptable Use Policy.

6. DATA PROTECTION RISKS

6.1 This policy helps to protect the College from some very real data security risks, including:

6.1.1 Breaches of confidentiality, for instance,

- information being given out inappropriately.
- employees not ensuring the screens of their computers are locked when left unattended.
- personal data shared informally, in particular when sent by email, as this form of communication is not secure, or over the phone.
- data not being encrypted before being transferred electronically.

6.1.2 Failing to offer choice. For instance, all individuals should be free to choose how the College uses data relating to them.

6.1.3 Reputational damage. For instance, the College could suffer if hackers successfully gained access to sensitive data.

7. DATA PROTECTION PRINCIPLES

7.1 When using Personal Data, Data Protection Laws require that the College complies with the following principles. These principles require Personal Data to be:

7.1.2 processed lawfully, fairly and in a transparent manner;
7.1.3 collected for specified, explicit and legitimate purposes and not further processed in manner that is incompatible with those purposes;
7.1.4 adequate, relevant and limited to what is necessary for the purposes for which it is being collected;
7.1.5 accurate and kept up to date, meaning that every reasonable step must be taken to ensure that Personal Data that is inaccurate is erased or rectified as soon as possible;
7.1.6 kept for no longer than is necessary for the purposes for which it is being processed; and
7.1.7 stored 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.

7.2 These principles are considered in more detail in the remainder of this Policy.

7.3 In addition to complying with the above requirements the College must also demonstrate in writing that it complies with them. The College has several policies and procedures in place, including this Policy and the documentation referred to in it, to ensure that the College can demonstrate its compliance. This is the concept of Accountability.

Lawful purposes for processing ordinary Personal Data

7.4 In order to collect and/or use Personal Data lawfully the College needs to be able to show that its use meets at least one of a number of legal grounds. These are set out in Article 6 of the GDPR and are as follows (paraphrased):

7.4.1 **Consent:** the individual has given valid consent for you to process their personal data for a specific purpose.

7.4.2 **Contract:** the processing is necessary to perform a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

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

7.4.4 **Vital interests:** the processing is necessary to protect someone's life.

7.4.5 **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.

7.4.6 **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 – in particular where they are a child.

1.1 More information about Lawful Basis can be found on the ICO website: A guide to lawful basis | ICO

Lawful purposes for Special Categories of Personal Data

7.5 There are additional conditions which need to be met in order to use Special Categories of Personal Data. These are set out in Article 9 and are as follows (paraphrased):

- explicit consent;
- employment and social security obligations;
- vital interests;
- necessary for establishment or defense of legal claims;
- substantial public interest; and
- various scientific and medical issues.

7.6 The College needs to ensure that for each type of Special Categories of Personal Data it processes, it has established one of the above legal bases for processing it. The following link provides more detail regarding these conditions: What are the conditions for processing? | ICO

7.7 The College has carefully assessed how it uses Personal Data and how it complies with the obligations set out above. If the College changes how it uses Personal Data, the College needs to update this record and may also need to notify individuals about the change. If College Personnel therefore intend to change how they use Personal Data at any point they must notify the Data Protection Officer who will decide whether their intended use requires amendments to be made and any other controls which need to apply.

Criminal Offence Data

7.8 There are additional conditions which need to be met in order to use Criminal Offence data. These are set out in Schedule 1 of the Data Protection Act 2018. These include, but are not limited to:

- Employment, social security and social protection
- Health or social care purposes
- Public health
- Preventing or detecting unlawful acts
- Preventing fraud
- Safeguarding of children and individuals at risk

1.2 The following link provides more detail regarding the conditions for processing Criminal Offence Data: Criminal offence data | ICO

7.9 The College will ensure that for every instance of law enforcement processing, it has established one of the above legal bases for processing it. If the College changes how it uses criminal offence data, the College will update this record and may also need to notify Individuals about the change. If College Personnel intend to change how they use Personal data at any point they must notify the Data Protection Officer who will decide whether their intended use requires amendments to be made and any other controls which need to apply.

8. TRANSPARENT PROCESSING – PRIVACY NOTICES

8.1 Wyke Sixth Form College aims to ensure that individuals are aware that their data is being processed. Where the College collects Personal Data directly from Individuals, the College will inform them about how the College uses their Personal Data. This is in a privacy notice. The College Privacy Notices can be found here: Policies

8.2 If the College changes how it uses Personal Data, the College may need to notify Individuals about the change. If College Personnel therefore intend to change how they use Personal Data, please notify the Data Protection Officer who will decide whether the College Personnel's intended use requires amendments to be made to the privacy notices and any other controls which need to apply.

9. DATA QUALITY – ENSURING THE USE OF ACCURATE, UP TO DATE AND RELEVANT PERSONAL DATA

9.1 Data Protection Laws require that the College only collects and processes Personal Data to the extent that it is required for the specific purpose(s) notified to the Individual in a privacy notice (see paragraph 8 above) and as set out in the College's record of how it uses Personal Data. The College is also required to ensure that the Personal Data the College holds is accurate and kept up to date.

9.2 All College Personnel that collect and record Personal Data shall ensure that the Personal Data is recorded accurately, is kept up to date and shall also ensure that they limit the collection and recording of Personal Data to that which is adequate, relevant, and limited to what is necessary in relation to the purpose for which it is collected and used. In practice, data should be held in as few places as necessary and staff should not create any unnecessary additional data sets.

9.3 All College Personnel that obtain Personal Data from sources outside the College shall take reasonable steps to ensure that the Personal Data is recorded accurately, is up to date and limited to that which is

adequate, relevant, and limited to what is necessary in relation to the purpose for which it is collected and used. This does not require College Personnel to independently check the Personal Data obtained.

9.4 In order to maintain the quality of Personal Data, all College Personnel that access Personal Data shall ensure that they review, maintain and update it to ensure that it remains accurate, up to date, adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. Please note that this does not apply to Personal Data which the College must keep in its original form (e.g. for legal reasons or that which is relevant to an investigation).

9.5 It is the responsibility of all Personnel to ensure that their details are up to date and accurate and to inform the College if any changes need to be made.

9.6 The College recognises the importance of ensuring that Personal Data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection Laws. The Rights of Individuals are included in this document in Section 15. This sets out how the College responds to requests relating to these issues.

10. PERSONAL DATA MUST NOT BE KEPT FOR LONGER THAN NEEDED

10.1 Data Protection Laws require that the College does not keep Personal Data longer than is necessary for the purpose or purposes for which the College collected it.

10.2 The College has assessed the types of Personal Data that it holds and the purposes it uses it for and has set retention periods for the different types of Personal Data processed by the College, the reasons for those retention periods and how the College securely deletes Personal Data at the end of those periods. These are set out in the Data Retention and Destruction Policy.

10.3 If College Personnel feel that a particular item of Personal Data needs to be kept for more or less time than the retention period set out in the Data Retention Policy, for example because there is a requirement of law, or if College Personnel have any questions about this Policy or the College's Personal Data retention practices, they should contact the Data Protection Officer for guidance.

11. DATA SECURITY

The College takes information security very seriously and the College has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. The College has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. The College has in place an IT and Internet Acceptable Use Policy which supports this Data Protection Policy.

12. DATA STORAGE

12.1 These rules describe how and where data should be safely stored. Questions about storing data safely should be directed to the Head of IT.

12.2 When data is stored on paper, it should be kept in a secure place where unauthorised people cannot gain access to it.

12.3 These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

12.3.1 When not being used but still required, the paper or files should be kept in a locked drawer or filing cabinet.
12.3.2 Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
12.3.3 Data printouts should be shredded and disposed of securely when no longer required.

12.4 When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

12.4.1 Data should be protected by strong passwords, and possible multi-factor authentication where available, that are changed regularly and never shared between employees.
12.4.2 Data should only be stored on designated drives and servers and should only be uploaded to approved cloud computing services.
12.4.3 Data should not be stored on removable media (e.g. USB pen drive, external hard drive, CD or DVD) unless absolutely necessary; if removable media devices are used to store data, these should be password protected, and kept locked away securely when not being used. The data should be removed from these as soon as it is no longer needed on the device.
12.4.4 Servers containing personal data should be sited in a secure location, away from general office space.
12.4.5 Data should be backed up frequently. Those backups should be tested regularly, in line with the College's standard backup procedures.
12.4.6 Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
12.4.7 All servers and computers containing data should be protected by approved security software and a firewall.

13. DATA BREACH

13.1 Whilst the College takes information security very seriously, unfortunately, in today's environment, it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of, or alteration of Personal Data. If this happens there will be a Personal Data breach and College Personnel must comply with the College's Data Breach Notification Procedure (see Appendix 3).

13.2 A Personal Data breach is defined very broadly and is effectively any failure to keep Personal Data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of Personal Data. While most Personal Data breaches happen as a result of action taken by a third party, they can also occur as a result of something someone internal does.

13.3 There are three main types of Personal Data breach which are as follows:

13.3.1 **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that a member of College Personnel is not authorised to access, accessing Personal Data stored on a lost laptop, phone or other device, people "blagging" access to Personal Data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong student, or disclosing information over the phone to the wrong person;

13.3.2 **Availability breach** - where there is an accidental or unauthorised loss of access to, or destruction of, Personal Data e.g. loss of a memory stick, laptop, phone or other device, denial of service attack, infection of systems by ransom ware, deleting Personal Data in error, loss of access to Personal Data stored on systems, inability to restore access to Personal Data from back up, or loss of an encryption key; and

13.3.3 **Integrity breach** - where there is an unauthorised or accidental alteration of Personal Data.

13.4 The College has a data breach procedure which can be seen in Appendix 3 of this document. This procedure outlines how the College will deal with a data breach and the timescales it will intend to meet. If you suspect a data breach, please consult this procedure and follow the steps outlined or email the Data Protection Officer at dpo@wyke.ac.uk

14. APPOINTING CONTRACTORS WHO ACCESS THE COLLEGE'S PERSONAL DATA

14.1 If the College appoints a contractor who is a Processor of the College's Personal Data, Data Protection Laws require that the College only appoints them where the College has carried out sufficient due diligence and only where the College has appropriate contracts in place.

14.2 One requirement of GDPR is that a Controller must only use Processors who meet the requirements of the GDPR and protect the rights of individuals. This means that data protection due diligence should be undertaken on both new and existing suppliers. Once a Processor is appointed, they should be audited periodically to ensure that they are meeting the requirements of their contract in relation to Data Protection.

14.3 Any contract where an organisation appoints a Processor must be in writing.

14.4 You are considered as having appointed a Processor where you engage someone to perform a service for you and as part of it, they may get access to your Personal Data. Where you appoint a Processor you, as Controller, remain responsible for what happens to the Personal Data.

14.5 GDPR requires the contract with a Processor to contain the following obligations as a minimum:

- to only act on the written instructions of the Controller;
- to not export Personal Data without the Controller's instruction;
- to ensure staff are subject to confidentiality obligations;
- to take appropriate security measures;
- to only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;
- to keep the Personal Data secure and assist the Controller to do so;
- to assist with the notification of Data Breaches and Data Protection Impact Assessments;
- to assist with subject access/individuals rights;
- to delete/return all Personal Data as requested at the end of the contract;
- to submit to audits and provide information about the processing; and
- to tell the Controller if any instruction is in breach of the GDPR data protection law.

14.6 In addition, the contract should set out:

- the subject-matter and duration of the processing;
- the nature and purpose of the processing;
- the type of Personal Data and categories of individuals; and
- the obligations and rights of the Controller.

14.7 In certain circumstances, the legislation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, the college may disclose requested data. However, we will ensure the request is legitimate, seeking assistance from the Corporation and from the college's legal advisers where necessary.

15. RIGHTS OF INDIVIDUALS

15.1 GDPR gives individuals more control about how their data is collected and stored and what is done with it. We will ensure that individuals can exercise their rights in the following ways:

15.2 **Right of Access** (Subject Access Requests)

15.2.1 Individuals have the right under the GDPR to ask the College to confirm what Personal Data they hold in relation to them and provide them with the data. This information has to be provided within the timescale of one month (with a possible extension of a further two months if it is a complex request). A fee cannot be charged for complying with the request. Appendix 4 describes the Subject Access Request procedure.

15.3 **Right of Erasure** (Right to be Forgotten)

15.3.1 This is a limited right for individuals to request the erasure of Personal Data concerning them where:

- the use of the Personal Data is no longer necessary;
- their consent is withdrawn and there is no other legal ground for the processing;
- the individual objects to the processing and there are no overriding legitimate grounds for the processing;
- the Personal Data has been unlawfully processed; and
- the Personal Data has to be erased for compliance with a legal obligation.

15.3.2 In a marketing context, where Personal Data is collected and processed for direct marketing purposes, the individual has a right to object to processing at any time. Where the individual objects, the Personal Data must not be processed for such purposes.

15.4 **Right of Data Portability**

15.4.1 An individual has the right to request that data concerning them is provided to them in a structured, commonly used and machine-readable format where:

- the processing is based on consent or on a contract; and
- the processing is carried out by automated means

15.4.2 This right isn't the same as subject access and is intended to give individuals a subset of their data.

15.5 **The Right of Rectification and Restriction**

15.5.1 Individuals are given the right to request that any Personal Data is rectified if inaccurate and to have use of their Personal Data restricted to particular purposes in certain circumstances.

15.6 **Right to be informed**

15.6.1 Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR.

15.6.2 The College provides Privacy Notices to individuals and groups to inform them of the purposes for processing their personal data, the retention periods for that personal data, and who it will be shared with.

15.7 **Right to restrict processing**

15.7.1 Individuals have the right to "block" or "suppress" the College's processing of their personal data when:

- they contest the accuracy of the personal data, for a period enabling the College to verify the accuracy of the personal data;
- the processing is unlawful, and the individual opposes the deletion of the personal data and requests restriction instead;
- the College no longer needs the personal data for the purposes the College collected it for, but the College is required by the individual to keep the personal data for the establishment, exercise or defence of legal claims;
- the individual has objected to the College's legitimate interests, for a period enabling the College to verify whether its legitimate interests override their interests.

15.7.2 If the College has disclosed the individual's restricted personal data to any third parties, the College is required to tell the individual who those third parties are and to inform the third parties about the restriction where the College can.

15.7.3 When an individual asks the College to restrict its processing of their personal data, the College is required to do so and to confirm to the individual in writing within one month of them making the request that this has been done.

15.8 **Right to object**

15.8.1 Individuals have the right to object to the College's processing of their personal data where:

- the College's processing is based on its legitimate interests or the performance of a task in the public interest and the individual has grounds relating to his or her particular situation on which to object;
- the College is carrying out direct marketing to the individual; and/or
- the College's processing is for the purpose of scientific/historical research and statistics and the individual has grounds relating to his or her particular situation on which to object.

15.9 **Rights related to automated decision making including profiling**

15.9.1 We must respect the rights of individuals in relation to automated decision making and profiling.

15.9.2 Individuals retain their right to object to such automated processing, have the rationale explained to them, and request manual intervention.

15.10 The College will use all Personal Data in accordance with the rights given to Individuals under Data Protection Laws and will ensure that it allows Individuals to exercise their rights under these laws.

16. MARKETING AND CONSENT

16.1 The College will sometimes contact Individuals to send them marketing or to promote the College. Where the College carries out any marketing, Data Protection Laws require that this is only done in a legally compliant manner.

16.2 Marketing consists of any advertising or marketing communication that is directed to particular individuals. When the College is marketing to individuals, we must ensure that we provide the following:

- Sufficient detail in our privacy notices, including for example whether profiling takes place; and
- Rules on obtaining consent are sufficiently strict and require an individual's "clear affirmative action". The ICO like consent to be used in a marketing context.

16.3 Consent is central to electronic marketing. The College will use an un-ticked opt-in box.

16.4 Alternatively, the College may use a “soft opt in” when the following conditions are met:

- contact details have been obtained in the course of a sale (or negotiations for a sale)
- the College are marketing its own similar services; and
- the College gives the individual a simple opportunity to refuse to opt out of the marketing, both when first collecting the details and in every message after that.

16.5 The College will adhere to the Privacy and Electronic Communications Regulations (PECR) which sits alongside the Data Protection Act and the UK GDPR. This applies to direct marketing, such as communications directed to particular individuals and covers any advertising/marketing material. It applies to electronic communication i.e. calls, emails, texts, faxes. PECR rules apply even when personal data is not being processed.

17. AUTOMATED DECISION MAKING AND PROFILING

17.1 Under Data Protection Laws there are controls around profiling and automated decision making in relation to Individuals.

- **Automated Decision Making** happens where the College makes a decision about an Individual solely by automated means without any human involvement and the decision has legal or other significant effects; and
- **Profiling** happens where the College automatically uses Personal Data to evaluate certain things about an Individual.

17.2 Any Automated Decision Making or Profiling which the College carries out can only be done once the College is confident that it is complying with Data Protection Laws. If College Personnel therefore wish to carry out any Automated Decision Making or Profiling College Personnel must inform the Data Protection Officer.

17.3 College Personnel must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Officer.

17.4 The College does not carry out Automated Decision Making or Profiling in relation to its employees.

18. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

18.1 The GDPR requires data controllers to carry out a risk assessment in relation to the use of Personal Data for any new service, product or process. This must be done prior to the processing via a Data Protection Impact Assessment (**"DPIA"**). A DPIA should be started as early as practical in the design of processing operations. A DPIA is not a prohibition on using Personal Data but is an assessment of issues affecting Personal Data which need to be considered before a new product/service/process is rolled out. The process is designed to:

- describe the collection and use of Personal Data;
- assess its necessity and its proportionality in relation to the purposes;
- assess the risks to the rights and freedoms of individuals; and
- the measures to address the risks.

18.2 A DPIA should be completed where the use of Personal Data is likely to result in a high risk to the rights and freedoms of individuals. The ICO's standard DPIA template is available from Information Commissioner's Office

18.3 Where a DPIA reveals risks which are not appropriately mitigated the ICO must be consulted.

18.4 Where the College is launching or proposing to adopt a new process, product or service which involves Personal Data, the College needs to consider whether it needs to carry out a DPIA as part of the project initiation process. The College needs to carry out a DPIA at an early stage in the process so that the College can identify and fix problems with its proposed new process, product or service at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

18.5 Where a DPIA identifies that a web-based College service is likely to be used by children we will also aim to ensure this complies with the Children's Code.

18.6 Situations where the College may have to carry out a Data Protection Impact Assessment include the following (please note that this list is not exhaustive):

- large scale and systematic use of Personal Data for the purposes of Automated Decision Making or Profiling (see definitions above) where legal or similarly significant decisions are made;
- large scale use of Special Categories of Personal Data, or Personal Data relating to criminal convictions and offences e.g. the use of high volumes of health data;
- introduction of a new IT system which processes large amounts of data: or
- systematic monitoring of public areas on a large scale e.g. CCTV cameras.

18.7 All DPIAs must be reviewed and approved by the Data Protection Officer.

19. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE UK

19.1 Data Protection Laws impose strict controls on Personal Data being transferred outside the UK. Transfer includes sending Personal Data outside the UK but also includes storage of Personal Data or access to it outside the UK. This should be considered whenever the College appoints a supplier outside the UK or the College appoints a supplier with group companies outside the UK which may give access to the Personal Data to staff outside the UK.

19.2 So that the College can ensure it is compliant with Data Protection Laws, College Personnel must not export Personal Data unless it has been approved by the Data Protection Officer.

19.3 College Personnel must not export any Personal Data outside the UK without the approval of the Data Protection Officer.

19.4 The College transfers personal information outside of the UK in the following circumstances: with the British Council and/or country of origin for international students

20. THE AGE-APPROPRIATE DESIGN CODE (THE CHILDREN'S CODE)

20.1 The College accepts and recognises that some of its web-based services are likely to be accessed by people under the age of 18. When this is the case particular emphasis and care must be taken to ensure compliance with the Age Appropriate Design Code (Children's Code).

20.2 Situations where this may apply include but are not limited to:

- The provision of online based support services, such as web portals and college emails
- Processing data in relation to submitting applications to enrol with the college
- The use of any apps developed or used officially by Wyke College that are likely to be used by under 18s
- The College will monitor the development and usage of its web-based platforms and add further examples where appropriate.

20.3 When the College identifies that a service is likely to be used by children, either by a DPIA or other means, we will ensure that this service is operated in the best interests of the child, this will be done by:

- Keeping them safe from exploitation risks, including the risks of commercial or sexual exploitation and sexual abuse;
- Protect and support their health and wellbeing;
- Protect and support their physical, psychological and emotional development;
- Protect and support their need to develop their own views and identity;
- Protect and support their right to freedom of association and play;
- Support the needs of children with disabilities in line with our obligations under the relevant equality legislation for England, Scotland, Wales and Northern Ireland;
- Recognise the role of parents in protecting and promoting the best interests of the child and support them in this task; and
- Recognise the evolving capacity of the child to form their own view and give due weight to that view.

- The College shall also ensure when providing a web-based service likely to be used by children that it follows the other principles of the age-appropriate design code should they be relevant to the service. These can be found on the ICOs website.

21. MONITORING AND REVIEW

21.1 This policy will be monitored by the Policy Review Group and Corporation and will be reviewed annually.

22. EQUALITY AND DIVERSITY

22.1 This policy has been reviewed to assure the promotion of equality on grounds of gender, gender reassignment, sexual orientation, race, religion or belief, disability, age, marriage and civil partnership, and pregnancy and maternity. The review deemed it to be compliant with the College's Equality and Diversity Policy.

23. RELATED COLLEGE DOCUMENTS

Documents related to this policy are:
Data retention and destruction policy
IT and Internet Acceptable Use Policy
Disciplinary Policy
Wyke AI Policy

Policy, procedure, practice or strategy:	**DATA PROTECTION POLICY**		
Person responsible:	Head of MIS	Date:	Dec 2025
Briefly describe the aims, objectives & purpose of this policy, procedure, practice or strategy.	The purpose of the document is to provide the College policy for compliance with the General Data Protection Regulation and the Data Protection Act 2018. The policy aims to outline the expectations for staff and students and personal data processing. Additionally, the policy identifies individual responsibilities of key members of staff and their role specifically associated with data protection.		
	Please ensure the following characteristics are considered when assessing the questions below along with any others you feel to be relevant: Gender, Sexuality, Transgenderism, Age, Race, Religion/belief, Disability, Marital/Civil partnership status, Pregnancy or maternity. Responses may be based on learner and staff data, complaints, feedback, research, student/staff surveys and/or professional judgement.		
Is there potential, or opportunity that the proposed policy, procedure, practice or strategy will affect any groups adversely (including possible discrimination) or positively?	None identified at this stage		
If any action is required as a result of this screening exercise please note them, along with any mechanisms for reviewing the impact of the policy, procedure or practice.	N/A		

Appendix 1 - Responsibilities of the Data Protection Officer

Reporting to Corporation Audit Committee

The Data Protection Officer will report annually to the Corporation Audit committee on Data Protection matters in the college, and more frequently should need arise.

The annual report will include:

- Update regarding significant changes in GDPR or related legislation, and how it may affect the college.
- An update of the Corporation's responsibilities under GDPR and related legislation.
- Any proposals for updates to this policy (The GDPR and Data Protection policy, and related policies).
- A summary of the quantity and scope of subject access requests made in the last year.
- An update report of staff training carried out in the year, and any potential requirements for whole staff training in the forthcoming year.

Review of Policies and procedures

All policies and procedures at Wyke Sixth Form College are subject to annual review by the manager responsible for them, reporting back either to the college Policy Review Group, or to the relevant committee of the Corporation.

This policy will be reviewed by the Data Protection Officer, who will report back and propose updates to the Audit Committee of the Corporation.

Training and advice

As part of the role, the Data Protection Officer:

- Will arrange appropriate data protection training as part of staff induction for staff covered by this policy.
- Where there is significant change in legislation, or identified training needs arise, arrange appropriate training for all staff.
- Will advise staff colleagues on data protection, and their responsibilities under the Act.

Dealing with Subject Access Requests

The Data Protection Officer is the first part of contact for subject access requests. They will:

- Create an entry in the SAR Log for each request.
- Investigate the request and identify the volume of work involved.
- Arrange for any collation of data in response to a request.
- Carry out all communications with the data subject on behalf of the College.
- Dispatch any response made by the college, maintaining the SAR log entries as appropriate
- Checking and approving agreements with third parties handling college sensitive data
- The Data Protection Officer must inspect all contracts and agreements involving third party processing or data sharing, advise on whether the college can safely commit to any such contract or agreement, and any necessary adjustments.

Appendix 2 - GDPR Responsibilities of Head of IT

The Head of IT will:

Ensure all systems, services and equipment used for storing data meet acceptable security standards

This will include the technological measures to:

- protect against potential data theft, whether on-site or in transit
- protect against third party deletion or alteration of personal data
- protect against data loss due to inadequate backups
- maintain a resilient infrastructure which helps ensure business continuity in the college

Perform regular checks and scans to ensure security hardware and software function properly

We will continue to develop tests to give the college early warning of potential threats to our infrastructure.

Evaluate any third-party services the College is considering using to store or process data. For instance, cloud computing service

Any third-party storage solution used within the college to store personal data must be approved by the Data Protection Officer (or whoever fulfils this role for the college).

In particular, care should be taken around authentication, use of SSL or encryption technology, and ensuring that the data remains within the European Economic Area (EEA).

Appendix 3 – Data Breach Procedure

Where there is a data breach within the College, it is a legal requirement to notify the ICO within 72 hours and the individuals concerned as soon as possible in certain situations. It is essential therefore that all data breaches, no matter how big or small, are reported to the Data Protection Officer.

This Procedure should be read in conjunction with Section 13 of this document, which contains information on what constitutes a data breach.

This Procedure should be followed by all staff. At all stages of this procedure, our Data Protection Officer and management will decide whether to seek legal advice. This procedure will also apply where we are notified by any third parties that process personal data on our behalf that they have had a data breach which affects our personal data.

The procedure is set out below. Any failure to follow this procedure may result in disciplinary action.

IDENTIFYING AND REPORTING A DATA BREACH

If you discover a data breach, however big or small, you must report this to our Data Protection Officer immediately. The Data Protection Officer is Rob Davey and can be contacted at: Tel. 01482 346347 ext 112, Email dpo@wyke.ac.uk

Any other questions about the operation of this procedure or any concerns that the procedure has not been followed should be referred in the first instance to the Data Protection Officer.

A data breach could be as simple as putting a letter in the wrong envelope and therefore even the most minor data breaches ***must*** be reported.

False alarms or even breaches that do not cause any harm to individuals or to the College should nevertheless be reported as it will enable us to learn lessons on how we respond and the remedial action we put in place.

We have a legal obligation to keep a register of all data breaches, no matter how big or small and no matter whether any harm was caused. Please ensure that you do report any breach, even if you are unsure whether or not it is a breach.

BECOMING AWARE OF A DATA BREACH – INVESTIGATING

We become aware of a data breach when we have a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. From this point, our time limit for notification to the ICO will commence.

When you report a data breach to our Data Protection Officer, our Data Protection Officer will promptly investigate the breach to ascertain whether we are fully aware that are breach has occurred that has led to personal data being compromised.

ASSESSING A DATA BREACH

Once you have reported a breach and our Data Protection Officer has investigated it and has decided that we are aware that a breach has occurred, our Data Protection Officer will log the breach in our Data Breach Register and will carry out an initial assessment of the breach to evaluate its severity.

Once the level of severity is known, our Data Protection Officer will notify management. If necessary, we will appoint a response team which may involve for example our HR and IT teams and we will assign responsibility for particular tasks as necessary across the response team.

We will then investigate the breach and consider any on-going risks to the College and any individuals affected.

If our Data Protection Officer and management consider that the breach is very serious, they will consider the impact on our reputation and the effect it may have on the trust placed in us. Our Data Protection Officer and senior management will consider whether to appoint a PR professional to advise on reputational damage and will also consider whether legal advice is needed.

FORMULATING A RECOVERY PLAN

Our Data Protection Officer and senior management will investigate the breach and consider a recovery plan to minimise the risk to individuals. As part of the recovery plan, our Data Protection Officer and senior management may interview any key individuals involved in the breach to determine how the breach occurred and what actions have been taken.

NOTIFYING A DATA BREACH TO THE ICO

Unless the breach is unlikely to result in a risk to the rights and freedoms of individuals, we must notify the breach to the ICO within **72 hours** of becoming aware of the breach. We must also notify the individuals concerned as soon as possible where the breach is likely to result in a high risk to their rights and freedoms.

The content of the notification will be drafted by our Data Protection Officer in line with our Data Breach Policy, and the notification will be made by our Data Protection Officer – please be aware that **under no circumstances must you try and deal with a data breach yourself**.

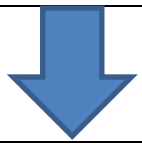
NOTIFYING A DATA BREACH TO INDIVIDUALS

We must also notify the individuals concerned as soon as possible where the breach is likely to result in a high risk to their rights and freedoms.

The content of the notification will be drafted by our Data Protection Officer in line with our Data Breach procedure and in conjunction with consulting the ICO if considered necessary. We will notify individuals in clear and plain

language and in a transparent manner (for example by email, SMS or letter). Please be aware that **under no circumstances must you try and deal with a data breach yourself.**

In some circumstances, we may not need to notify the affected individuals. Our Data Protection Officer will decide whether this is the case.



NOTIFYING A DATA BREACH TO OTHER RELEVANT THIRD PARTIES

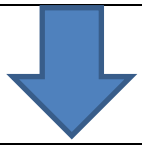
We may also consider that it is necessary to notify other third parties about the data breach depending on the nature of the breach. This could include:

- Insurers
- Police
- Employees
- Parents/Guardians
- Sponsors
- Banks
- Contract counterparties

The decision as to whether any third parties need to be notified will be made by our Data Protection Officer and management. They will decide on the content of such notifications.

CONSIDER WHETHER NOTIFICATIONS NEED TO BE UPDATED

We need to keep the ICO up to date about the data breach. If anything changes from the time we send the initial notification to the ICO, our Data Protection Officer will consider whether we need to update the ICO about the data breach.



EVALUATION AND RESPONSE

The key to preventing further incidents is to ensure that the College learns from previous incidents.

It is extremely important to identify the actions that the College needs to take to prevent a recurrence of the incident. Our Data Protection Officer and management will carry out an evaluation as to the effectiveness of our response to the data breach and document this in our Data Breach Register.

Appendix 4 – Subject Access Request – policy and procedure

1. All individuals who are the subject of personal data held by the college are entitled to:
   - Ask **what information** the college holds about them and why.
   - Ask **how to gain access** to it.
   - Be informed **how to keep it up to date.**
   - Be informed how the College is **meeting its data protection obligations**.

   If an individual contacts the college requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to the data controller at *subjectaccess@wyke.ac.uk.* The college can supply a standard request form, although individuals do not have to use this.

   The college will always verify the identity of anyone making a subject access request before handing over any information. The following information will be required to confirm the identity of the data subject before any information can be provided:
   - Full Name
   - Date of Birth
   - Student Number or Staff Number

   The College may also require proof of identity, in which case the following forms of ID will be acceptable:
   - Birth Certificate
   - Passport
   - Driving License

   In the first instance, all subject access requests should be forwarded to the Data Protection Officer (or designated individual acting in the role in their absence).

   The college will reserve the right to take further steps to satisfy itself of the identity of anyone requesting data.

2. On receipt of a subject access request:
   - The request will be logged in the Subject Access Log spreadsheet.
   - The request will initially be assessed by the Data Protection Officer to determine how the College should respond.
   - A response acknowledging receipt of the request will be sent to the person requesting the data.
   - Any data recovered will be dispatched in electronic form in the first instance. The data will be encrypted, and the encryption key will be dispatched separately.
   - The College will act to protect the data of data subjects at all times and may take further steps to establish confidence that the data is being sent to the person lawfully entitled to receive it before sending personal data.