# DATA PROTECTION POLICY

| | |
|---|---|
| **Role responsible:** | Vice-Principal (Finance, Resources & Systems) |
| **Author:** | Director of Network & Information Systems |
| **Approved by:** | Corporation |
| **Date Approved:** | **Approved by the Corporation: 22 May 2018** |
| **Next Review Date:** | |
| **Publication:** | MS Teams |
| **Changes made:** | |

# Data Protection Policy

## Purpose

Wyke Sixth Form College needs to gather and use certain information about individuals.

These can include applicants, students, parents or guardians, staff, suppliers, business contacts and other people the college has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the college's data protection standards, and to comply with the law.

This data protection policy ensures that the college:

- Complies with data protection law and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

## Data protection law

The General Data Protection Regulations (GDPR) (EU 2016/679), which succeeds the 1998 Data Protection Act, describes how organisations such as Wyke Sixth Form College must collect, handle and store personal information.

The GDPR applies to **personal data** meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

Article 5 of the GDPR requires that personal data shall be:

- **processed lawfully, fairly and in a transparent manner** in relation to individuals;

- **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;

- **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed;

- **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;

- **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; and

- **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.**

Article 5(2) requires that the data controller (Wyke Sixth Form College) shall be responsible for, and be able to demonstrate, compliance with the principles.

## Equality statement

This policy applies to all college staff regardless of age, race, disability, religion or belief, gender, sexual orientation, marital or civil partnership status, gender reassignment, pregnancy or maternity, or any other status. All individuals will be treated in a fair and equitable manner recognising any special needs where adjustments can be made. No individual will suffer any form of unlawful discrimination, victimisation, harassment or bullying as a result of this policy.

## Status of the Policy

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by rules and policies made by the College. 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.

## Data protection risks

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

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the College uses data relating to them.
- **Reputational damage.** For instance, the College could suffer if hackers successfully gained access to sensitive data.

## Responsibilities

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.

Each employee who handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

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

- 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

- 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.

- The Director of Networks and Information Systems 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.

Further details of GDPR responsibilities of the Data Protection Officer can be found in **Appendix One.**

Further details of GDPR responsibilities of the Director of Network and Information Systems can be found in **Appendix Two.**

## General staff guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- **The College will provide regular training** to all employees to help them understand their responsibilities when handling data.

Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

- In particular, **strong passwords must be used** and they should never be shared.
- College data **should not be disclosed** to unauthorised people, either within the College or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

## Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Digital Technologies Manager or Director of Network and Information Systems.

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

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

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

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

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the College's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

## Data use

Personal data is of no value to the college unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The Director of Network and Information Systems can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area** without prior approval of the Senior Management Team.
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

## Data accuracy

The law requires the college to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a student's details when having discussions. Student data can be updated through the MIS Office.
- The college will seek to make it **easy for data subjects to update the information** we about them. For instance, via the College website.
- Data should be **updated as inaccuracies are discovered**. For instance, if a student can no longer be reached on their stored telephone number, it should be removed from the database.

## Personal Data Breach

A 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. This includes breaches that are the result of both accidental and deliberate causes. If a member of staff or student believes a breach has taken place, they should contact the Data Protection Officer immediately.

On becoming aware of a data breach a full investigation will be completed by the Data Protection Officer who will contain the situation, assess the potential adverse consequences for individuals, recover the breach if possible and report to the ICO where appropriate within 72 hours. Any individual affected by a significant breach will be informed including the measures taken to mitigate any possible adverse effects.

Any security incident will be investigated to determine if the breach was a result of human error, a system error or of a malicious nature. Further staff training and revisions to systems may take place as identified following the investigation. All staff are aware that any breach of the General Data Regulations Policy may result in the college's disciplinary procedures being instigated.

Actions to be taken in the event of a security breach may be found in the College IT Security Policy.

## Subject access requests

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.

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).

Subject access requests from individuals can be made by email, addressed to the data controller at *subjectaccess@wyke.ac.uk.*

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

On receipt of a subject access request:

1. The request will be logged in the Subject Access Log spreadsheet

2. The request will be initially assessed by the Data Protection Officer to determine how the college should respond

3. A response acknowledging receipt of the request will be sent to the person requesting the data

4. 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 seek to use an alternative communication channel to send this key (e.g. via SMS to a known mobile phone number).

5. The college will act to protect the data of data subjects at all time, 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.

## Disclosing data for other reasons

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 will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the Corporation and from the college's legal advisers where necessary.

## Providing information

Wyke Sixth Form College aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the college has a privacy statement for students, applicants and staff, setting out how data relating to individuals is used by the college. This is available on request. A version of this statement is also available on the college website.

## Student Obligations

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, contact details etc. are notified to the MIS Office or Tutor as soon as is possible.

## Retention of Data

The College will keep some forms of information for longer than others. Because of storage problems, information about students cannot be kept indefinitely, unless there are specific

requests to do so. Appendix 3 contains archiving guidelines and retention times currently employed by the College.

# Appendix One: 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)
- 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 reporting 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
- Despatch 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 Two

## GDPR Responsibilities of Director of Networks and Information Systems

The Director of Network and Information Systems 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 Three : Retention of Data

Wyke Sixth Form College seeks to retain personal data for no longer than is necessary. Full details are available in the College Information Audit Register.

Examples of retention periods for different classes of data at time of writing are as follows:

| | |
|---|---|
| Safeguarding information | 6 years – but longer if in connection with serious safeguarding issue |
| Open Event (Sign in) | Deleted each year in October (max 1 year) |
| Safeguarding information | 6 years – but longer if in connection with serious safeguarding issue |
| Liaison Events | To be removed following events. |
| Paper application Forms | Paper records destroyed once inputted into system these records then To be kept on student file – 6 years. |
| Record of Exam entries and UCIs | To be kept on student file – 6 years. |
| Special considerations seating plans and private candidates | 12 months following the student leaving the college. |
| Staff new starter forms / change of details forms / leaver forms– other pay related information, sickness, etc. / monthly salary paperwork | Up to date as per HRMC guidelines of 7 years. |
| Information relating to bursary students and the management of their funds, bus passes, clothing etc. | To be kept on student file – 6 years. Archiving procedure now in place with NRS for the trust e-info |
| User account Active Directory data | Current academic year + 1 year. |
| User data | Current academic year + 1 year |
| Application form (where subsequently enrolled) (includes personal details, medical and learning disability declarations, ethnic origin, nationality, predicted QoE) Note – Single Year application forms contains additional information on progress, grades, tutor comments etc. | To be kept on student file – 6 years. |
| Applicant details (where not subsequently enrolled) | Deleted in October after the academic year for which the application was made |
| Enrolment form (based on application and pre-enrolment data already provided, also includes parental consent, Dr's details) Note – Y2 re-enrolment form contains additional information on progress, grades, tutor comments etc. | To be kept on student file – 6 years. |
| Residence evidence | To be kept on student file – 6 years. |

**Approved by the Corporation, 22 May 2018**