# DATA PROTECTION POLICY

| | |
|---|---|
| Policy Title: | DATA PROTECTION POLICY |
| Issue Date (m/y): | 05/2018 – Updated 09/22 |
| Author(s): | Vice Principal |
| Approved by: | Senior Management Team |
| Date of Equality Assessment: | 09/2022 |
| Review date: | 09/2023 |
| Related Policies and Procedures: | Freedom of Information Policy<br>GDPR Documents including Retention Schedule, Breach Procedure, Information Sharing Agreement, DPIA, Lifecycles, Asset Register, Staff Guidance Notes |

Equality Impact Assessment Tool

Name of Policy: Data Protection Policy

| | | Yes/No | Comments |
|---|---|---|---|
| 1 | Does the policy/guidance affect one group less or more favourably than another on the basis of: | No | |
| | Race or ethnicity | No | |
| | Disability | No | |
| | Gender | No | |
| | Religion or belief | No | |
| | Sexual orientation | No | |
| | Age | No | |
| | Marriage and Civil Partnership | No | |
| | Maternity and Pregnancy | No | |
| | Gender Reassignment | No | |
| 2 | Is there any evidence that some groups are affected differently? | No | |
| 3 | If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable? | N/A | |
| 4 | Is the impact of the policy/guidance likely to be negative/ | No | |
| 5 | If so, can the impact be avoided? | N/A | |
| 6 | What alternatives are there to achieving the policy/guidance without the impact? | N/A | |
| 7 | Can we reduce the impact by taking different action? | N/A | |

# Contents

## 1. INTRODUCTION

Suffolk New College is committed to a policy of protecting the rights and privacy of individuals including students, staff and other individuals in contact with the College, in accordance with the General Data Protection Regulation (GDPR) May 2018.

The new regulatory environment demands higher transparency and accountability in how colleges manage and use personal data. It also accords new and stronger rights for individuals to understand and control that use.

The GDPR contains provisions that the College must adhere to as a Data Controller, including provisions intended to enhance the protection of an individual's personal data. For example the GDPR requires that we must ensure that College Privacy Notices are written in a clear, plain way that students, staff, and other individuals will understand.

Suffolk New College needs to process certain information about individuals with whom it has a relationship with for various purposes including but not limited to:

- The recruitment and payment of staff
- The administration of programmes of study and courses
- Processing student enquiries, applications, enrolment and alumni information
- The administration of examinations and external accreditation
- Recording student progress, attendance and conduct
- Collecting fees
- Complying with legal obligations to funding bodies and government including local government
- Provision of facilities, services and support as part of a contract of learning or employment
- The provision of commercial services and facilities for internal and external parties
- The creation of marketing materials and learning content

To comply with various legal obligations, including the obligations imposed on it by GDPR, Suffolk New College must ensure that information about individuals is collected and used fairly, stored safely and securely, is not disclosed to any third party unlawfully, and only retained for as long as necessary.

More information can be obtained from the Information Commissioner's Office (ICO) if required.

A comprehensive set of all of the College's key documents related to this Policy and the GDPR can be found on the College Staff Intranet 'Information Management' page:

Link (Staff intranet) : https://livesuffolkac.sharepoint.com/sites/Intranet/SitePages/Information-Management.aspx

Link (Staff intranet) : https://livesuffolkac.sharepoint.com/sites/Intranet/SitePages/Data-Protection-Overview.aspx

## 1.1 COMPLIANCE

This policy applies to all staff and students of Suffolk New College. Any breach of this policy or of the Regulation itself will result in action being taken under the College's Staff Disciplinary Procedures or Supporting Student Achievement Policy.

As a matter of best practice, other agencies and individuals working with Suffolk New College who have access to personal information will be expected to read and comply with this policy.

It is required that departments who are responsible for dealing with external bodies with whom personal information of individuals is shared, will take the responsibility for ensuring that such bodies sign a contract which among other things, will include an agreement to abide by this policy. This may take the form of GDPR compliance clauses in a new contract, an addendum to an existing contract, or a specific Information Sharing Agreement.

This policy will be updated as necessary to reflect best practice in data management, security and access controls, and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

## 1.2 TERMINOLOGY

**Personal Data -** data which relates to a living individual who can be identified. The College is required to process relevant personal data regarding members of staff, volunteers, applicants, parents, students, alumni and customers as part of its operation and shall take all reasonable steps to do so in accordance with this Policy.

**Sensitive Personal Data** – The College may, from time to time, be required to process sensitive personal data. Sensitive personal data includes data relating to medical information, religion, race or ethnicity, sexual orientation, criminal records and proceedings. This data will only be connected with records for staff and students where it is needed to meet some contractual or legal requirement. If the data is gathered for statistical analysis, it will be separated from the main record and made anonymous.

**The Data Subject -** The person identified, or who can be identified from the personal data or, when used in conjunction with other data held by the data controller, or data that is likely to come into their possession.

**The Data Controller –** The College as a Body Corporate is the Data Controller under the Act, and the Corporation is therefore ultimately responsible for compliance.

**The Designated Data Controller** – is responsible for day-to-day Data Protection issues and coordination. The College's identified designated Data Controller is Mary Gleave, Vice Principal. The Data Controller is assisted by:

- The Head of Human Resources for staff and payroll matters.

- The Clerk to Corporation for Corporation Members
- The Funding & Performance Manager for student records and systems
- The Director of Safeguarding & Student Support for student support and library services
- The Director of IT Services for general IT security and compliance issues
- The Head of Estates & Facility Management for physical security, building access control and monitoring systems.

The Designated Data Controller will endeavor to ensure that all personal data is processed in compliance with this Policy and the Principles of the GDPR 2018. The Freedom of Information Act 2000 and the Protection of Freedoms Act 2012 are also relevant to parts of this policy.

**Processing** - means obtaining, recording or holding the information or carrying out an operation on the information.

**Recipient** - any person or party to whom the data is disclosed, including another staff member other than the Data Controller.

**Source** - a recognised and lawful source of personal data collection.

**Disclosure** – the process of providing personal data to a recognised and lawful recipient (in compliance with the purpose of processing).

**Information Commissioner's Office** – ICO, Government body responsible for overseeing the Data Protection legislation.

Link (ICO Website): https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

## 1.3 GENERAL DATA PROTECTION REGULATION (GDPR)

The legislation came into force from 25th May 2018. GDPR regulates the processing of personal data, and protects the rights and privacy of all living individuals (including children); for example, by giving all individuals a general "right of access" to the personal data which relates to them, individuals can exercise the right to gain access to their information by means of a 'subject access request'.

Personal data may be in hard or soft copy (paper files, electronic records, photographs, CCTV images), and may include facts or opinions about a person.

The Data Protection Act sets out specific rights for College students in relation to educational records held within the state education system. These rights are set out in separate educational regulations 'The Education (Pupil Information) (England) Regulations 2005'.

Link: http://www.legislation.gov.uk/uksi/2005/1437/contents/made

For more detailed information on these Regulations see the Data Protection Data Sharing Code of Practice (DPCoP) from the Information Commissioner's Office (ICO):

https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

The College will review updates and amendments to these regulations and codes of practice as they relate to the GDPR.

## 1.4 RESPONSIBILITIES

The College will be the 'Data Controller' under the terms of the legislation. This means the College is ultimately responsible for controlling the use and processing of the personal data. The College also has a nominated governor who oversees this Policy and an Annual Report is shared with the Audit & Risk Committee, including details of any personal data breaches which have been reported.

The Executive Team and Business Support Management Team are responsible for day-to-day data protection matters (with a central point of contact/coordination role provided by the College's Designated Data Controller), and will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling practice within the College.

The Head of Estates & Facility Management is responsible for ensuring that the College's ICO Data Protection registration is up-to-date. The College's data registration number is Z7412859. Details of the College's registration can be found on the Office of the Information Commissioner's website.

Link: https://ico.org.uk/ESDWebPages/Entry/Z7412859

Compliance with the legislation is the personal responsibility of all members of the College who may process personal information.

Individuals who provide personal data to the College are responsible for ensuring that the information is accurate and up-to-date.

If an individual believes that the College has not complied with this Policy or acted otherwise, then in accordance with the GDPR, they should utilise the College Grievance Procedure (if a staff member) or Complaints Procedure (if a student, parent, guardian or member of the public). They may also raise the issue with the Designated Data Controller.

### STAFF OBLIGATIONS

- Ensuring that any information that they provide to the College in connection with their employment is accurate and up to date.
- Informing the College of any changes to this information or updating their records directly using any provided self-service facilities.
- Informing the College of any errors in their personal data that they become aware of.
- Periodically checking for updates to the Staff Data Privacy Notice, to ensure that they are aware of what personal information the College is collecting about them and the purposes it is being used for, etc.

If and when, as part of their responsibilities, staff collect information about other people, (e.g. about students' course work, opinions about ability, references to other academic institutions, or

details of personal circumstances), they must comply with the guidelines for staff, as detailed on the staff intranet.

Link (Staff intranet): https://livesuffolkac.sharepoint.com/sites/Intranet/SitePages/Information-Resources.aspx

**STUDENT OBLIGATIONS**

Student obligations are similar in that they must ensure that the personal data they provide to the College is accurate and up-to-date. They must inform the College of changes to their personal data, or if there are errors which they are aware of. However, they will be informed of any changes to the College's Student Privacy Notice by tutors, the student intranet or other methods.

## 2. DATA PROTECTION PRINCIPLES

The legislation places a responsibility on every Data Controller to process any personal data in accordance with the following eight principles. More detailed guidance on how to comply with these principles can be found on the ICO website.

**Link: (ICO Website):** https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles

The principles are as follows:

### 2.1 To process personal data fairly and lawfully

The College will make all reasonable efforts to ensure that individuals who are the focus of the personal data (Data Subjects) are informed of the identity of the Data Controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant to safeguarding their rights under the GDPR.

### 2.2 To process the data for the specific and lawful purpose for which it collected that data and not further process the data in a manner incompatible with this purpose.

The College will ensure that the reason for which it collected the data originally is the only reason for which it processes the data, unless the individual is informed of any additional processing before it takes place.

### 2.3 To ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed.

The College will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind, and if any irrelevant data are given by individuals, it will be destroyed immediately.

### 2.4 To keep personal data accurate and, where necessary, up to date.

The College will review personal information records periodically for accuracy, for example, during re-enrolment of continuing students. It is the responsibility of the individuals giving their

personal data to ensure that it is accurate, and each individual should notify the College if, for example, a change in circumstances means that the data needs to be updated. It is the responsibility of the College to ensure that any notification regarding the change is noted, and take reasonable steps to make corrections where possible.

**2.5 To only keep personal data for as long as is necessary.**

The College undertakes not to retain personal data for longer than is necessary to ensure compliance with legislation and other statutory requirements; for example, financial regulations and employment law. With regard to some core student data, the College will retain data to provide a historical source of data for internal analysis of the College's performance and impact on the region/community, to serve the public interest, and to aid in the planning of future curriculum and skills development programmes.

The College will undertake a regular review of the information held, and implement a process to destroy or anonymise personal information which has reached end of the retention period, in line with the College's Retention Schedule.

Where historical data is used for statistical or analytic purposes, it will be anonymised as part of the process before presentation in any report to protect the privacy of individuals.

The College will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste).

**2.6 To process personal data in accordance with the rights of the data subject under the legislation.**

Individuals have various rights under the legislation including a right to:

- Be informed of the nature of the information the College holds and any parties to whom this may be disclosed.
- Prevent processing likely to cause damage or distress.
- Prevent processing for purposes of direct marketing.
- Be informed about the mechanics of any automated decision-making process that will significantly affect them.
- Not have significant decisions that will affect them taken solely by an automated process.
- Sue for compensation if they suffer damage by any contravention of the legislation.
- Take action to rectify, block, erase or destroy inaccurate data.
- Request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened.

The College will only process personal data in accordance with individuals' rights, whilst taking into account the limits of these rights and/or additional emphasis placed on these rights in the GDPR in certain scenarios.

**2.7 To put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data.**

All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties.

The College will ensure that all personal data is accessible only to those who have a valid reason for using it.

The College has in place appropriate security and data protection measures, for example:

- Keeping all filed personal data in a lockable cabinet with key-controlled access.
- Physical building security with restricted access to tutor and administration workstations and paper-file handling areas, IT Server/Communications rooms, Examination and HR Records storage locations.
- Standard IT industry security and backup measures such as internet firewalls, anti-virus/spam systems, internet filtering and encryption of web services, tape and disk backup systems.
- Password protecting personal data held electronically.
- Placement of any PCs/Screens, CCTV camera monitoring screens etc., that may display personal data, such that they are not visible except to authorised staff.
- Training and awareness guidance to ensure that staff implement 'Data Safety' practices.
- Role Based Access Control (RBAC) to control access to shared database and data storage systems.

In addition, the College has in place appropriate measures for the deletion of personal data – manual records are shredded or disposed of as 'confidential waste' and appropriate contract terms will be put in place with any third parties undertaking this work. PCs disposed of or recycled have their hard disks securely wiped or destroyed.

This policy, and the data safety guidance also applies to staff and students who process personal data 'off-site', e.g. when working at home, or on personal devices, and in such circumstances additional care must be taken regarding the security of the data.

**2.8 To ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights freedoms of data subjects in relations to the processing of personal data.**

When putting in place new systems and services, the College will not transfer data to such territories without first conducting a Data Privacy Impact Assessment (DPIA) which will include seeking alternative solutions to keep that data within the EEA.

Under limited circumstances, such as using personal information for marketing purposes on the College's website, transfers of personal information may occur if the access attempt to the College website is made outside of the EEA. In this specific scenario, personal information used for marketing purposes will be processed only with the consent of the individual.

## 3. STATUS OF THE POLICY

It is a condition of employment that staff will abide by the rules and policies made by the College from time to time. Any failure to follow the policy can therefore result in disciplinary proceedings.

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 Controller for staff initially. If the matter is not resolved it should be raised as a formal grievance.

## 4. PERSONAL INFORMATION PRIVACY NOTICES

All individuals have the right to know about their personal data and how it will be used.
Any documentation which gathers personal and/or special categories of personal data should contain a web link to the College's Data Privacy Notices, or at least a copy or summary of the relevant notice ensuring that the following information is provided:

- Explanation of who we are
- What we will do with their data
- Who we will share it with, at least by category/type of organisation
- How long we will keep it for
- That their data will be treated securely
- If applicable, how to opt out of processing in some cases, or how to give consent to the processing in others
- Where they can find a copy of the full notice and who to contact with questions about privacy issues

A set of Privacy Notices covering the range of individuals and scenarios involved with the College can be found on the College's website, including students, staff, individuals recorded for marketing purposes, and visitors/clients of the College's commercial services.

Link: www.suffolk.ac.uk/privacy

### 4.1 Additional Notice for Students at Enrolment

The College will include the specified statement from the DfE on the Student Enrolment Form

and update as necessary following the ESFA's (Education and Skills Funding Agency) technical guidance:

*How We Use Your Personal Information*

*This privacy notice is issued by the Education and Skills Funding Agency (ESFA), on behalf of the Secretary of State for the Department of Education (DfE). It is to inform learners how their personal information will be used by the DfE, the ESFA (an executive agency of the DfE) and any successor bodies to these organisations. For the purposes of the Data Protection Act 2008, the DfE is the data controller for personal data processed by the ESFA. Your personal information is used by the DfE to exercise its functions and to meet its statutory responsibilities, including under the Apprenticeships, Skills, Children and Learning Act 2009 and to create and maintain a unique learner number (ULN) and a personal learning record (PLR).*

*Your information may be shared with third parties for education, training, employment and well-being related purposes, including for research. This will only take place where the law allows it and the sharing is in compliance with the Data Protection Act 2008.*

*The English European Social Fund (ESF) Managing Authority (or agents acting on its behalf) may contact you in order for them to carry out research and evaluation to inform the effectiveness of training.*

*You can opt out of contact for other purposes by ticking any of the following boxes if you do not wish to be contacted:*

- *About courses or learning opportunities*
- *For surveys and research*
- *By post*
- *By phone*
- *By email*

*Further information about use of and access to your personal data, and details of organisations with whom we regularly share data are available at:*

*https://www.gov.uk/government/publications/esfa-privacy-notice*

## 5. CHANGES TO CONSENT AS A BASIS FOR PROCESSING

The College understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement (e.g. via an enquiry form, or in an 'optional' section of the application/enrolment form) whilst being of a sound mind and without having any undue influence exerted upon them. Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.

Under the GDPR, obtaining consent to process personal data has more stringent rules and rights afforded to the Data Subject, including the right to withdraw consent at any time. This is in part to the misuse of consent historically under the Data Protection Act.

Therefore, the College will limit the use of consent as a legal basis for processing personal data, and will instead use 'performance of a contract' (i.e. an employment contract or learning agreement), or where the College has a 'legitimate interest' (i.e. processing a student application to meet enrolment targets) or or 'compliance with a law or regulation' (i.e. anti-fraud checks for payment processing), and in some cases where we are protecting the vital interest of an individual or individuals (i.e. obtaining next-of-kin for emergency contact purposes).

Consent will therefore be used in specific circumstances where no other legal basis can be applied. Examples include:

In the case where a specific individual or group of known individuals will be photographed for marketing purposes or learning content creation.

Or collecting information in order to respond to an enquiry from a prospective student or member of the public about a potential course, job post, or commercial service (such as a booking enquiry for the Sports Centre or Restaurant) provided by the College.

Consent will also be used when collecting personal information for optional activities that are not part of a learning or employment contract; for example, collecting information about sports and interests in order to help the College plan events and activities to improve the student/staff experience.

Consent may also be used when collecting contact information for marketing purposes of College services, programmes and business engagement activities.

The College will ensure that if the individual does not give his/her consent for the processing and there is no other lawful basis on which to process the data, then steps will be taken to ensure that processing of that data does not take place.

### 5.1 Other instances where consent will not apply

Agreement to the College processing some specified classes of personal data is a condition of acceptance by a student onto any course, and a condition of employment for staff. Both of these are considered to be contracts. This includes information about previous criminal convictions in accordance with the Rehabilitation of Offenders Act 1974.

Similarly, some jobs or courses will bring applicants into contact with children, including young people (children) between the ages of 14 and 18. The College has a duty to ensure that staff are suitable for the job and students are suitable for the courses offered. The College also has a duty of care to all staff and students, and must therefore make sure that staff and those who use the College facilities do not pose a threat or danger to other individuals. A refusal to sign the relevant documentation will result in the offer being withdrawn.

The College will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. The College will only use the information in the protection of the vital interest (health and safety) of the individual, for example in emergencies where the individual is incapacitated and unable to volunteer this information to Emergency Response personnel.

## 6. DATA SECURITY

The College will take appropriate technical and organisational steps to ensure the security of personal data. Some of these steps have already been mentioned in this Policy.

All staff will be made aware of this policy and their duties under the Act, with online training and guidance notes provided on the Staff Intranet. Similar guidance is available to students on the Student website and in awareness and induction programmes.

All staff and students are required to respect the personal data and privacy of others and must ensure that appropriate personal protection and security practices are adopted to protect against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to personal data.

All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely.
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.
- Care is taken to preserve access to personal information – for example, by being careful about accidentally erasing or losing personal information.

Staff should note that intentional unauthorised disclosures will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

To emphasise, personal information should be:

- kept in a locked filing cabinet; or
- in a locked drawer; or
- if it is computerised, be password protected; or
- kept only on a storage device which is itself secure – in most cases by using encryption.

Staff should refer to the staff guidance notes in this regard in particular the “Data Safety” guidance note provided on the Staff Intranet.

## 7. RIGHT OF ERASURE

Data Subjects have the right in some circumstances to request that information about them is erased, primarily when the purposes for the processing of that information no longer apply. This does not apply in all cases, for example, where records of mistakes or corrections are kept, or records which must be kept in the interests of all parties to which they apply.

There may also be other contractual, legal and regulatory limitations that apply to the right of erasure in specific scenarios.

The College will keep a record of any erasures that take place including a summary of the reason why it was requested. This is required by the ICO.

## 8. SUBJECT ACCESS REQUESTS (SARs)

Staff and students and other users of the College have the right to access any personal data which are being kept about them either on computer or in certain files. Any person who wishes to exercise this right should complete the College "Subject Access Request" forms for Staff or Students as appropriate.

A general Subject Access Request form is provided on the College's website for public use.

Link: www.suffolk.ac.uk/privacy

When making a request, individuals will need to prove their identity and may be asked to provide additional clarification about the nature and scope of their request before processing can begin.

If the College finds that a SAR it manifestly unfounded or excessive, or made repetitively, it may choose to charge for or refuse the request. A charge may also be incurred if additional copies of data are required. When deemed necessary, the charge will be £10 per request.

The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 30 calendar days unless there is good reason for a delay. In such cases, the reason for delay will be explained in writing to the Data Subject making the request, and any partial information available will be shared.

A record of any subject access requests is kept by the Designated Data Controller.

A copy of the College's Subject Access Request handling process flowchart is available for the public on request.

### 8.1 Data Portability

The College also acknowledges the right to Data Portability, which provides that an individual has the right to obtain a copy personal information that they themselves provided to the College in electronic format, such that they can transfer their information elsewhere. Subject to the limits on this right provided by the GDPR, including the scope/nature of personal data this applies to, and evaluation of the technical feasibility of complying with the request, the College will make reasonable effort to comply with this right.

## 9 EXEMPTIONS

Certain data is exempted from the provisions of the GDPR which includes the following: -

- National security and the prevention or detection of crime.
- The assessment of any tax or duty.
- Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the College, including Safeguarding and prevention of terrorism and radicalisation.

The above are examples of some of the exemptions under the Act. Any further information on exemptions should be sought from the Designated Data Controller.

## 10. DISCLOSURE OF DATA

Only disclosures which comply with the College's procedures, including ensuring up-to-date Information Sharing Agreements or GDPR-compliant contract clauses are in place, can be made and therefore staff should exercise caution when asked to disclose personal data held on another individual or third party.

The College undertakes not to disclose personal data to unauthorised third parties.

Legitimate disclosures may occur in the following instances:

- the individual has given their consent to the disclosure
- the disclosure is in the legitimate interests of the individual and/or the College
- the disclosure is required for the performance of a contract
- there is a legal reason for making the disclosure
- the disclosure is in the vital interest of the Data Subject or another party for example their next-of-kin

Under no circumstances will the College sell any of its databases to a third party.

## 11. PUBLICATION OF COLLEGE INFORMATION

It is the College policy to make as much information public as possible, and in particular the following personal data will be available to the public for inspection:

- Names of College Corporation Members and Register of Interests information relating to Corporation Members and senior staff with significant financial responsibilities (for inspection during office hours only).
- List of staff
- Photographs of Senior Postholders and Corporation Members.
- Information on examination results
- Photos and information in marketing materials
- Event information

The College's internal phone list will not be a public domain.

Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the Designated Data Controller or relevant department.

## 12. EMAIL COMMUNICATION

It is the policy of Suffolk New College to ensure that senders and recipients of email are made aware under the GDPR, and Freedom of Information legislation, the contents of email may have to be disclosed in response to a request for information. One means by which this will be communicated will be by a disclaimer on the College's email.

Under the Regulation of Investigatory Powers Act 2000, Lawful Business Practice Regulations, any email sent to or from the College may be accessed by someone other than the recipient for system management and security purposes.

## 13. CCTV RECORDING

There are some CCTV systems operating within the College for the purpose of protecting users of the College buildings and College property. This is a legitimate interest of the College.

The College will only process personal data obtained by the CCTV system in a manner which ensures compliance with the legislation. See the College's CCTV policy for more information and also the College's Retention Schedule for the period images are kept for.

## 14. EXAMINATION MARKS

Students are entitled to information about their marks for both coursework and examinations if available from the Awarding Body. However, this may take longer than other information to provide. The College may withhold references in the event that the full course fees have not been paid, or all books and equipment have yet to be returned to the College.

## 15. RETENTION OF DATA

The College keeps some forms of information for longer than others. The College's complete Statement of Records Retention is available on request and is published internally for staff awareness and process alignment purposes; it includes information on a range of different categories of information that the College holds and how long they are kept for.

## 16. BREACHES OF INFORMATION

It is the responsibility of all staff to notify the Data Protection Controller if a breach has occurred. Breaches may also be discovered by students or other individuals and reported to the College via a staff member or a direct report to the Designated Data Controller.

The definition of a breach, is any instance where personal information has been shared with an individual or organisation who has no authorised access to that information, or exposed to access by unlimited individuals, or any loss of access to such personal information, including physical loss or accidental erasure.

A general security measure to safeguard the security of personal data within the College are the confidentiality clauses within Employment Contracts which require all staff to treat all information with care and to not disclose data outside of the College or to unauthorised individuals within the College.

Therefore, if personal data of any type or form is discovered or accidentally accessed by an employee of a nature that they are not sure if they are authorised to normally access, line managers should be informed immediately such that a review and checks on systems, processes and access permissions can be made, and dependent upon severity of impact, the College's formal Breach Procedure can be initiated.

For any breaches which take place externally, please refer immediately to the College's formal Breach Procedure, with particular reference to the Breach Flowchart which provides details on the process to be undertaken. The College has 72 hours to determine the nature of the breach, any implications and impacts, potential notification of the impacted individual(s) and the ICO and actions put in place to mitigate against any identified risks.

The College keeps a record of any breaches which have taken place and these are reported to the College's Audit and Risk Committee on an annual basis.

A copy of the College's Data Breach Handling Process flowchart is available for the public on request.

## 17. CONCLUSION

Compliance with the General Data Protection Regulation (GDPR) May 2018 is the responsibility of all members of the College. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or access to College facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated College Data Controller.

## 18 SUPPORTING DOCUMENTATION

The College's public website privacy page contains our Privacy Notices, Data Protection Policy, Subject Access Request form and Freedom of Information policy and request form.

Link: www.suffolk.ac.uk/privacy

The College's staff intranet contains an aray of documentation:

Link: https://livesuffolkac.sharepoint.com/sites/Intranet/SitePages/Data-Protection-Overview.aspx

An Information Management Map depicting how the College's Information Management documentation supports our Data Protection and Freedom of Information policies can be found on the staff intranet and a copy has been provided below:

# Information Management Documentation Map