MidKent College Group
Data Protection Policy

APPROVED VERSION

Document Details			
Policy Number		**No. of Appendices**	**0**
Document Title	**Data Protection Policy 2024 - 2026**		
Document Description	Midkent College and Midkent Training Services Data Protection Policy		
Effective Date	**January 2024**	**Review Date**	**January 2026**
Version Number	**V3.0**	**Review Cycle**	**2 Years**
Document Status	**Approved**	**New Policy**	**No**
Contact Details	The contact details for the College's and the subsidiary company's Data Protection Officer are: Data Protection Officer, MidKent College, Medway Campus, Medway Road, Gillingham, Kent, ME7 1FN E-Mail: Data.Protection@midkent.ac.uk		

Document Authorisation				
	Authorisation Required	**Initial and Role**	**Digital Signature**	**Date**
Author	Yes	HF – Data Protection Officer	Hazel Foreman	5 Nov 23
Owner	Yes	CH – Executive Director for Employers and Corporate Services	Chris Hare	6 Nov 23
SLT Review	Yes	N/A		
Exec Approver	Yes			
GB Sub Committee	Yes – GR&A for major updates			
Full GB Committee	Yes – if required			

Policy Cross References - This policy should be read in conjunction with any other associated policies, with particular reference to	
Policy Name	**Policy Number**
Safeguarding Policy	
ICT Policies	
CCTV Policy	
Freedom of Information Policy	
Personal File Access and HR Records Retention	
Staff Code of Conduct	
Disciplinary Policy	
Homeworking Policy	
Remote Learning Policy	

Document Revision History		
Version Number	**Date**	**Summary of Revision**
V2.0	13/01/2022	Minor Changes to Job titles and addition of item (reference 4.1, page 10) in reference to data minimalization.
V3.0	12/10/2023	Minor Changes ➢ Review cycle changed to every 2 years ➢ Amendment Subject access request diligence 8.2

CONTENTS

1 INTRODUCTION 6
2 SCOPE 6
3 DEFINITIONS 6
4 DATA PROTECTION PRINCIPLES 10
4.1 PRINCIPLES A-D 10
4.2 PRINCIPLE (E) – RETENTION AND DESTRUCTION OF RECORDS 10
4.3 PRINCIPLE (F) – INFORMATION SECURITY 11
4.4 WORKING OFF-SITE 12
5 LAWFULNESS OF PROCESSING 12
5.1 CONSENT 12
5.2 DIRECT MARKETING 13
6 SPECIAL CATEGORIES OF DATA 13
7 CRIMINAL CONVICTIONS PERSONAL DATA 14
8 DATA SUBJECTS RIGHTS 14
8.1 THE RIGHT TO BE INFORMED 16
8.2 THE RIGHT OF ACCESS 16
8.3 THE RIGHT TO RECTIFICATION 17
8.4 THE RIGHT TO ERASURE 17
8.5 THE RIGHT TO RESTRICT PROCESSING 17
8.6 THE RIGHT TO DATA PORTABILITY 17
8.7 THE RIGHT TO OBJECT 17
8.8 RIGHTS IN RELATION TO AUTOMATED DECISION MAKING AND PROFILING 18
9 CONTROLLERS AND PROCESSORS 18
10 INTERNATIONAL DATA TRANSFERS 19
10.1 TRANSFERS ON THE BASIS OF AN ADEQUACY DECISION 19
10.2 PRIVACY SHIELD 19
10.3 TRANSFERS SUBJECT TO APPROPRIATE SAFEGUARDS 19
11 DATA SHARING 20
11.1 INTERNAL DATA SHARING 20
11.2 EXTERNAL DATA SHARING 21
11.3 SHARING STUDENT'S DATA WITH THOSE WHO HAVE PARENTAL RESPONSIBILITY OR ACT IN LOCO PARENTIS 22
11.4 LAW ENFORCEMENT AGENCIES AND EMERGENCY SERVICES REQUESTS 23
11.4.1 EMERGENCY INFORMATION REQUESTS (VITAL INTERESTS) 23
11.4.2 NON-EMERGENCY INFORMATION REQUESTS 24
12 ACCOUNTABILITY, ROLES AND RESPONSIBILITIES 24
12.1 DATA PROTECTION OFFICER (DPO) 24
12.2 INFORMATION GOVERNANCE GROUPS 25
12.3 INFORMATION GOVERNANCE TEAM (SHARED SERVICE) 26

12.4 GOVERNING BODY AND BOARD OF DIRECTORS 26
12.5 EXECUTIVE DIRECTORS 26
12.6 SENIOR LEADERSHIP TEAM AND COLLEGE LEADERSHIP TEAM 27
12.7 SENIOR MANAGER RESPONSIBLE FOR ICT 27
12.8 SENIOR MANAGER RESPONSIBLE FOR HUMAN RESOURCES (HR) 28
12.9 SENIOR MANAGER RESPONSIBLE FOR MANAGEMENT INFORMATION SYSTEMS (MIS) 28
12.10 EMPLOYEES AND INDIVIDUALS WORKING ON BEHALF OF THE COLLEGE AND SUBSIDARY COMPANY 28
12.11 STUDENTS AND LEARNERS 29
13 DATA PROTECTION BY DESIGN AND DEFAULT 29
13.1 RECORDS MANAGEMENT 30
13.2 DATA PROTECTION IMPACT ASSESSMENT 31
14 DATA BREACHES 31
15 POLICY MONITORING, REVIEW AND EVALUATION 33
16 EQUALITY IMPACT ASSESSMENT 33
17 POLICY DISTRIBUTION 33

1 INTRODUCTION

- MidKent College ("the College") and MKC Training Services Limited ("subsidiary company") are committed to data protection and acknowledge the "rights and freedoms" of all stakeholders and those with whom the College and its subsidiary company works with.

- This policy sets out the accountability and responsibilities of the College, subsidiary company, employees, contractors, agency staff, volunteers, students and other relevant parties, in ensuring compliance with data protection and the security of personal data as required under any and all applicable legislation. This includes, but is not limited to;

    - UK GDPR (United Kingdom General Data Protection Regulation)
    - Data Protection Act 2018
    - Freedom of Information Act 2000
    - Equality Act 2010
    - Computer Misuse Act 1990
    - Fraud Act 2006 (with regards to phishing and identity theft and fraud)
    - Theft Act (with regards to electronic theft)
    - Network and Information Systems and Regulations 2018
    - Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)
    - Investigatory Powers Act 2016 (which replaces the Regulation of Investigatory Powers Act 2000)

2 SCOPE

- This policy applies to data as stipulated under the UK GDPR, with particular reference to Article 2 and 3.

- MidKent College is an exempt charity under the Part 3 of the Charities Act 2011. The College is registered with the ICO under number Z6528598.

- MKC Training Services Limited is a wholly owned subsidiary of MidKent College. MKC Training Services Limited is registered with the ICO under number Z352117X.

- For the purposes of this policy, the College and the subsidiary company holds and processes personal data about individuals, including, but not limited to, employees, governors, directors, contractors, suppliers and partners, students, visitors, alumni and commercial clients.

3 DEFINITIONS

- "Data protection legislation" encompasses the UK GDPR and Data Protection Act 2018.

- “All other applicable legalisation” encompasses the legislation referenced under section 1 Introduction.

- The terms “supervisory authority” and “the commissioner” means the Information Commissioner’s Office (ICO).

- “All employees and individuals working on behalf of the College and the subsidiary company” encompasses the following: employees, contractors, agency staff and volunteers.

- “Records management” is defined by ISO 15489-1:2016(en) as “Field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.”

- Where applicable, and unless otherwise stated, all other terminology used in this policy relates to the legal definitions outlined under Article 4 of the UK GDPR as follows:

    1. *‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*

    2. *‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;*

    3. *‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future;*

    4. *‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;*

    5. *‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and*

organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

6. *'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;*

7. *'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;*

8. *'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;*

9. *'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with domestic law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;*

10. *'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;*

    (10A) 'public authority' and 'public body' are to be interpreted in accordance with section 7 of the 2018 Act and provision made under that section

11. *'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;*

12. *'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;*

13. *'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;*

14. *'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique*

identification of that natural person, such as facial images or dactyloscopic data;

15. *'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;*

16. *'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;*

17. *'representative' means a natural or legal person established in the United Kingdom who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;*

18. *'enterprise' means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;*

19. *'group of undertakings' means a controlling undertaking and its controlled undertakings;*

20. *'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established in the United Kingdom for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;*

21. *(21A) foreign designated authority' means an authority designated for the purposes of Article 13 of the Data Protection Convention (as defined by section 3 of the 2018 Act) by a party, other than the United Kingdom, which is bound by that Convention;*

22. *information society service' means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (1) [as it has effect immediately before IP completion day];*

23. *'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.*

24. *'third country' means a country or territory outside the United Kingdom;*

25. *references to a fundamental right or fundamental freedom (however expressed) are to a fundamental right or fundamental freedom which continues to form part of domestic law on and after IP completion day by virtue of section 4 of the European Union (Withdrawal) Act 2018, as the*

right or freedom is amended or otherwise modified by domestic law from time to time on or after IP completion day.]

4 DATA PROTECTION PRINCIPLES

- The College's and the subsidiary company 's processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the UK GDPR.

- The College and the subsidiary company are committed to upholding the data protection principles. All personal data under the College's and the subsidiary company's control will be processed in accordance with the principles.

- To demonstrate commitment to practically and operationally upholding these principles, the College and the subsidiary company publishes and maintains an Information Charter. The Information Charter operates concurrently with all other policies and procedures.

4.1 PRINCIPLES A-D

A. Lawfulness, fairness, and transparency
B. Purpose Limitation
C. Data Minimisation
D. Accuracy

- The College and the subsidiary company will implement all reasonable measures to maintain compliance with the above principles.

- All data must be collected and processed lawfully, fairly, and transparently.

- May only collect data for specified explicit, and legitimate purposes that have been made clear to data subjects at the start of the processing.

- The college and the subsidiary company are required to ensure that adequate, relevant, and limited data is used where necessary in relation to the purposes for which they are processed. All data collection should be minimised.

- Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

4.2 PRINCIPLE (E) – RETENTION AND DESTRUCTION OF RECORDS

- The College and the subsidiary company will not keep personal data in a form that permits identification of data subjects for a longer period than is

necessary, in relation to the purpose(s) for which the data was originally collected.

- The College and the subsidiary company reserve the right to store data for longer periods if the personal data is processed solely for archiving purposes in the public interest, statistical purposes, scientific or historical research purposes, or if necessary to fulfil contractual obligations. This is subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

- The retention period for each category of personal data will be set out in the Retention Schedule along with the criteria used to determine this period including reference to any statutory obligations.

- When disposing of personal data, the College and the subsidiary company will:

    - only delete or dispose of data in line with the Retention Schedule, or in response to a right of erasure request where the conditions set out in Articles 17 and 19 of the UK GDPR are met.
    - ensure that paper-based records are shredded or disposed of by the approved contractors.
    - ensure that hard drives are destroyed by approved contractors as the College and the subsidiary company do not have the facilities to do so to the required standard in house. The disposal of hard drives should also comply with the Waste Electrical and Electronic Equipment Regulations 2013.
    - appoint contractors responsible for data destruction that, at a minimum, meet the criteria identified as being necessary to meet the legal requirements, in addition to data protection legislation, and all other applicable legalisation.
    - review the criteria for the disposal of personal data prior to the commencement of any applicable contracts.

4.3 PRINCIPLE (F) – INFORMATION SECURITY

- The College and the subsidiary company continuously seek to develop and implement measures that ensure a high level of security for personal and confidential data and to maintain a secure environment for information held both manually and electronically.

    - The security measures applied are listed in the College's ICT Policies.

- All personal data should be accessible only to those who need to use it, with access granted in line with the remits of an individual's job role or in accordance with data subject rights.

- All paper-based personal data is to be kept in rooms with key locks or centralised access control, and stored in locked units including, but not limited to, lockable drawers, filing cabinets and cabinets.

- All electronically held data is processed as per the details contained within the College's ICT Policies.

    - The controls listed in the College's ICT Policies are applied on the basis of identified risk to personal data, and the potential for damage or distress to individuals whose data is being processed.

4.4 WORKING OFF-SITE

- The College and the subsidiary company understand that data protection is not a barrier to working offsite and data protection legislation does not prevent this. However, the processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data and requires the implementation of measures to reduce the risk(s).

- The College and the subsidiary company must be satisfied that employees have adequate security measures in place for this to happen. Refer to Homeworking Policy (MidKent College staff) or Flexible Working Policy (Subsidiary company staff).

5 LAWFULNESS OF PROCESSING

- Any personal data processed by the College and the subsidiary company must be done so in accordance with one of the six lawful bases defined in Article 6 of the UK GDPR.

- In order for the College and the subsidiary company to fulfil their obligations and business requirements, the most appropriate lawful basis must be identified for each task. The lawful basis must be documented in the Records of Processing Activities as per Article 30 of the UK GDPR.

- The processing of special category data is covered under section 6 Special Categories of Data.

- The College and the subsidiary company accept that no matter how urgent the data collection, processing or sharing is, the Article 6 of the UK GDPR lawful basis, and any associated conditions, must be identified, met and documented beforehand. Failure to do so is a breach of the data protection legislation, and significantly increases the risks to data subject's rights and freedoms.

- In accordance with the Equality Act 2010, the College and the subsidiary company acknowledges that data subjects can reserve the right to not disclose personal data relating to protected characteristics.

5.1 CONSENT

- The College and the subsidiary company recognise that for consent to be valid as lawful basis, the requirements of Articles 6-8 of the UK GDPR must be met. The College and the subsidiary company acknowledge that when using consent as a lawful basis, the data subject must have the option to easily withdraw their consent.

5.2 DIRECT MARKETING

- The College and the subsidiary company will only send electronic direct marketing communications where it is the recipient's choice to opt-in.

- The College and the subsidiary company will ensure that in all electronic direct marketing communications the recipient will have the option to opt-out. If a recipient withdraws consent, the College and the subsidiary company will action as appropriate.

- The College and the subsidiary company will only send direct marketing in accordance with data protection legislation and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR).

6 SPECIAL CATEGORIES OF DATA

- The College and the subsidiary company understand that special category data is personal data which requires additional protection because it is sensitive and poses the greatest risk to individuals' risk and freedoms if compromised.

- Article 9 of the UKUK GDPR defines the ten special categories of data as personal data pertaining to an individual's:

    - racial or ethnic origin;
    - political opinions;
    - religious or philosophical beliefs;
    - trade union membership;
    - genetic data;
    - biometric data (where used for identification purposes);
    - health;
    - sex life; and
    - sexual orientation.

- Any special category data processed by the College and the subsidiary company must be done so in accordance with an identified lawful basis under Article 6 of the UK GDPR and a separate condition for processing identified under Article 9 UK GDPR.

- In addition to the requirements listed in Article 9 of the UK GDPR, under Part 1 and 2 of Schedule 1 of the Data Protection Act, if the College and the subsidiary company relies on condition:

- (b), (h), (i) or (j) the College and the subsidiary company acknowledge that the associated conditions and safeguards need to be met before processing the data.
- (g) the College and the subsidiary company acknowledge that one of 23 specific substantial public interest conditions set out need to be met before processing the data.
- (b) or (g) the College and the subsidiary company are required to complete an 'appropriate policy document' before processing the data.

- The College and the subsidiary company accept that no matter how urgent the requirement is to collect, process or share special category data, the Article 6 and 9 of the UK GDPR lawful bases, and any associated conditions, must be identified, met and documented beforehand. Failure to do so is a breach of the data protection legislation, and significantly increases the risks to data subject's rights and freedoms.

- The College and the subsidiary company will take measures to ensure that special category data is necessary for the purposes identified and that there is no other reasonable and less intrusive way to achieve that purpose.

- If the College and the subsidiary company cannot suitably identify, and justify, why special category data is required, the College will not proceed with the processing.

7 CRIMINAL CONVICTIONS PERSONAL DATA

- The College and the subsidiary company understand that information pertaining to criminal convictions is personal data; and no matter how urgent the need is for criminal convictions data to be collected, processed or shared, additional protections are required because of the sensitivity and increased risk to individuals' rights and freedoms if compromised.

- Prior to processing criminal convictions data, the College and the subsidiary company will identify and document accordingly:

    - the applicable condition from Article 10 of the UK GDPR and identity if it is processing the data in an official capacity or under a condition in Schedule 1 of the Data Protection Act 2018;
    - the lawful basis from Article 6 and 9 of the UK GDPR;
    - how it is complying with the Rehabilitation of Offenders Act 1974 (ROA) and Disclosure and Barring Service (DBS).

- If the College and the subsidiary company cannot suitably identify, and justify, why criminal convictions data is required, the College will not proceed with the processing.

8 DATA SUBJECTS RIGHTS

- The College and the subsidiary company acknowledge that it must comply with the eight rights set out in Articles 12-23 of the UK GDPR to data subjects, known as “Data Subjects Rights”:

    - The right to be informed - The right to be told how personal data is used in clear and transparent language.
    - The right of access, also known as a data subject access request (DSAR) - The right to know and have access to the personal data held about the individual.
    - The right to rectification - The right to have personal data corrected where it is inaccurate or incomplete.
    - The right to erasure, also known as the right to be forgotten - The right to have personal data deleted.
    - The right to restrict processing - The right to limit the extent of the processing of the individual’s personal data.
    - The right to data portability - The right to receive personal data in a common and machine-readable electronic format.
    - The right to object - The right to complain and to seek to prevent the processing of an individual’s data.
    - Rights in relation to automated decision making and profiling - The right not to be subject to decisions without human involvement.

- The College and the subsidiary company are committed to facilitating requests made by data subjects meeting the criteria of the above rights. As such, the College and the subsidiary company will:

    - process personal data in a transparent manner.
    - uphold individuals’ rights under data protection legislation and allow data subjects to exercise their rights over the personal data held about them.
    - keep records of all requests and their outcome.
    - respond to requests made under these rights based on the conditions set out in law. Not all the data subjects’ rights are absolute, and depending on the circumstances, exemptions may apply.
    - instruct employees receiving any requests made in relation to data subjects’ rights, to not directly respond, and refer the request to the Data Protection Team. This is supplemented by additional reminders about this requirement during employee induction and data protection training.
    - maintain internal procedures that detail how to process each of the data subject rights.
    - take reasonable measures to require individuals to confirm their identity where it is not obvious that they are the data subject.
    - not charge a fee to data subjects for enacting these rights, unless a request is found to be “manifestly unfounded or excessive” and/or reserves the right to refuse requests that are “manifestly unfounded or excessive”.
    - strive to respond to all requests made by data subjects under Articles 15-22 of the UK GDPR (rights 2-8) as per Article 12 (3) which specifies the legal timeframe as *“…without undue delay and in any event within*

one month of receipt of the request". If a request is complex then the College and the subsidiary company will invoke its ability to extend the deadline by a further 2 months, pursuant to the legislative requirements being met. However, in addition to the above, as per Article 12 (4) of the UK GDPR, when extreme mitigating circumstances arise that hinder the College and the subsidiary company from meeting these obligations, the College and the subsidiary company will consult with data subjects and seek advice from the ICO about how to proceed. This includes but is not limited to; unforeseen/major disasters that affect operations in line with business continuity and disaster recovery operations.
    - review all requests made under data subjects rights on a case by case basis but will apply a consistent approach.

- Failure to provide information requested as part of a response to a data subject rights request is considered to be a breach of this policy and will be dealt with under the relevant Disciplinary Policy.

- If as a result of responding to a data subject rights request it is identified that a breach of policy has occurred, the matter will be dealt with under the relevant Disciplinary Policy.

8.1 THE RIGHT TO BE INFORMED

- The College and the subsidiary company are committed to processing personal data in a transparent manner as per Articles 12-14 of the UK GDPR. To this end, the College and the subsidiary company will produce privacy notices that:

    - acknowledges the data subjects' rights;
    - explains how individuals can exercise their rights;
    - are available in a variety of accessible forms,
    - use clear, plain, meaningful language; and
    - provide all relevant information required under Article 12 of the UK GDPR and the ICO guidelines.

8.2 THE RIGHT OF ACCESS

- The College and the subsidiary company are committed to providing data subjects access to data held about them as per Articles 12 and 15 of the UK GDPR. To this end, the College and the subsidiary company:

    - recognises that it is a criminal offence to delete personal data relevant to a right to access request after it has been received. The College and the subsidiary company are committed to only securely disposing of personal data in line with the Retention Schedule or in response to a right to erasure request where the qualifying circumstances apply.
    - take all reasonable measures to not adversely affect the rights and freedoms of others when responding to DSARs.

- accept a subject access request verbally or in writing. When a request is made verbally the College and the subsidiary company may ask the data subject to follow this up in writing when a request is unclear.
- The college will request confirmation of the data subjects ID and required diligence before undertaking any requests and releasing data.
- will provide all relevant information required under Article 12 and 15 of the UK GDPR and the ICO guidelines.

8.3 THE RIGHT TO RECTIFICATION

- The College and the subsidiary company are committed to ensuring that as the personal data held about data subjects is accurate, in accordance with the lawful bases upon which it is collected, and where applicable, the corresponding retention period defined in law. This is done so in accordance with Articles 12 and 16 of the UK GDPR. To this end, the College:

    - will take reasonable measures to ensure that personal data remain accurate, but this is dependent on the data subject providing current and correct information.
    - will work with data subjects to rectify inaccuracies swiftly when errors are identified.

8.4 THE RIGHT TO ERASURE

- Pursuant to Articles 17 and 19 of the UK GDPR the College and the subsidiary company will delete personal data when one or more the following conditions within Article 17 of the UK GDPR are met.

8.5 THE RIGHT TO RESTRICT PROCESSING

- Pursuant to Articles 18 and 19 of the UK GDPR the College and the subsidiary company will restrict the processing of personal data when one or more the following conditions within Article 18 of the UK GDPR are met.

8.6 THE RIGHT TO DATA PORTABILITY

- Pursuant to Article 20 of the UK GDPR the College and the subsidiary company will provide personal data in a secure, structured, commonly used, and machine-readable format when one or more the following conditions within Article 20 of the UK GDPR are met.

8.7 THE RIGHT TO OBJECT

- Pursuant to Article 21 of the UK GDPR the College and the subsidiary company will stop the processing of their personal data when one or more the following conditions within Article 20 of the UK GDPR are met.

8.8 RIGHTS IN RELATION TO AUTOMATED DECISION MAKING AND PROFILING

- Pursuant to Article 22 of the UK GDPR the College and the subsidiary company will ensure that it fulfils its obligations when the conditions within Article 20 of the UK GDPR are applicable.

- If the College and the subsidiary company relies upon automated decision making and profiling, the process(es) will be subject to intense scrutiny and risk assessments to ensure that there are no alternative solutions available and that data subject rights are upheld.

9 CONTROLLERS AND PROCESSORS

- Primarily, the College and the subsidiary company are considered data controllers for personal data processed in line with operational requirements and are therefore responsible for establishing policies and procedures which ensure compliance with legislation.

- For the purposes of Government funding and performance accountability, the College shares data with (and may act on behalf of) external agencies. Principally this is the Department for Education and any executive agencies it sponsors, for example the Education and Skills Funding Agency (ESFA). In these situations, the external agency acts as a data controller in their own right.

- For the purposes of fulfilling contractual obligations, the subsidiary company shares data with (and may act on behalf of) external agencies. Principally this is with other parties subject to the same contract. In these situations, the external agency acts as a data controller in their own right.

- The College and the subsidiary company will only appoint processors if, and when, sufficient guarantees around compliance with the data protection legislation have been supplied.

- Where a processor can demonstrate that they adhere to approved codes of conduct or certification schemes, the College and the subsidiary company will take this into consideration for choice of supplier.

- Processors, working with or for the College and the subsidiary company, who have access to personal data, will be expected to comply with this policy.

- When the College and the subsidiary company uses a processor, a written contract/agreement with compulsory terms as set out in Article 28 of the UK GDPR must be in place, along with any additional requirements that the College and the subsidiary company determines necessary. Any written contracts/agreements with processors will entail a clause that specifies that processors can only act on the instruction of the College and the subsidiary

company also giving the College and the subsidiary company the right to audit compliance with the agreement.

10 INTERNATIONAL DATA TRANSFERS

- The College and the subsidiary company will only transfer data outside the UK in accordance with Articles 44-50 of the UK GDPR.

10.1 TRANSFERS ON THE BASIS OF AN ADEQUACY DECISION

- The College and the subsidiary company will refer to the list of countries/territories that the UK has deemed as covered by an 'adequacy regulation' before transferring personal data.

10.2 PRIVACY SHIELD

- In accordance with the judgment in the Schrems II case issued by the European Court of Justice on Thursday 16 July 2020, the College and the subsidiary company will not use the Privacy Shield framework to transfer personal data to the United States.

10.3 TRANSFERS SUBJECT TO APPROPRIATE SAFEGUARDS

- Should the College and the subsidiary company identify the need to transfer data to a third country that does not have an adequacy rating, the College will review each case independently against the criteria and options listed in Article 46 of the UK GDPR.

- The College and the subsidiary company will approach the transfer of personal data to third counties using an exemption with extreme caution and will not rely on the exemptions listed lightly, and never routinely.

- The College and the subsidiary company will only transfer personal data to third counties once:

    - all the appropriate documentation has been completed, including DPIAs;
    - the conditions set out in Chapter 5 (Articles 44-50) of the UK GDPR have been met; and
    - the transfer has been approved by the DPO.

- The College and the subsidiary company will determine which mechanism in Article 46 of the UK GDPR is adequate for the College and the subsidiary company to use, based on the following factors:

    - the nature of the information being transferred;
    - the country or territory of the origin, and final destination, of the information;
    - how the information will be used and for how long;

- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
- the security measures that are to be taken as regards the data in the overseas location.

11 DATA SHARING

- The College and the subsidiary company must ensure that personal data is not disclosed to unauthorised parties including, but not limited to, a data subject's family members and/or friends, government bodies, and in certain circumstances, law enforcement agencies.

- Individuals appointed in an official capacity to work on behalf of the College and the subsidiary company should exercise caution when asked to disclose personal data held on another individual to a third party and are expected to seek support from the Data Protection Officer.

- In all cases (regardless of whether they are internal or external), before data is shared, the College and the subsidiary company will:

    - consider whether it is appropriate to anonymise or pseudonymise the data first. The decision outcome should be documented, including the supporting arguments.
    - ensure that all necessary precautions to maintain the security, integrity and proper treatment of personal data have been considered and documented. If, based on the information provided, the College and the subsidiary company cannot guarantee that the recipient, whether it is an internal or external party, adequately complies with data protection legislation then the College and the subsidiary company will refuse to provide the data and/or sign any contracts/agreements.
    - where possible and appropriate, seek the data subject's consent prior to any sharing or disclosure beyond the purpose it was collected for. Personal data may be shared without the subject's consent in the following circumstances:

        - In the vital interests of the data subject or another person.
        - Where the data subject lacks capacity and the data is being shared with a legal guardian.
        - Under court order or for the purposes of law enforcement; refer to section 14.4 Law Enforcement and Emergency Services Requests.
        - Seeking legal advice or representation.
        - For the purposes of providing a confidential reference in the interests of the data subject.
        - In order to comply with a legal obligation.
        - In order to comply with requirements defined as being in the public interest.

11.1 INTERNAL DATA SHARING

- When personal data is shared internally, the recipient must only process the data in a manner consistent with the original purpose for which the data was collected.

- If personal data is shared internally for a new and different purpose, the Data Protection Officer must be consulted first. In these circumstances, consideration must be given to:

    - whether the data sharing is congruent with the lawful basis upon which the data was collected to do so;
    - determine if the data subjects need to be consulted or consent to the processing;
    - determine if the data needs to be re-collected for the new purpose;
    - if any additional documentation is required, including a new privacy notice.

11.2 EXTERNAL DATA SHARING

- When personal data is shared externally, a record of the request and whether the request was approved or denied will be recorded. If approved the nature of the data disclosed and details of the lawful basis identified, along with any supporting paperwork required, including but not limited to, data protection impact assessments and appropriate policy documents must be recorded. It is important that on each occasion data is shared externally that is considered in regard to the lawful basis upon which it was collected.

- When sharing data externally one or more of the following signed documents are required between the College/subsidiary company and the third party to define the obligations of both parties:

    - a data sharing agreement
    - a contract, which includes sufficient reference to data protection,
    - a non-disclosure agreement
    - a confidentiality agreement

- The above signed documents do not apply if disclosure is required by law enforcement agencies, including but not limited to, requests from the Department for Work and Pensions or Inland Revenue, or the third party requires the data for law enforcement purposes. In these circumstances the Law Enforcement Information Sharing Procedure; refer to section 14.4 Law Enforcement and Emergency Services Requests.

- There are some third parties with which the College and the subsidiary company shares information on a regular basis. This includes to external agencies under which the College may be obliged to share personal information relating to an individual to fulfil statutory obligations. Data subjects are made aware of these organisations prior to the data sharing taking place, via privacy notices.

- The College and the subsidiary company reserve the right to request and review any and all documentation necessary for assessing whether a third party adequately complies with data protection legislation this includes, but is not limited to, privacy notices and data protection policies.

11.3 SHARING STUDENT'S DATA WITH THOSE WHO HAVE PARENTAL RESPONSIBILITY OR ACT IN LOCO PARENTIS

- Section 11.3 applies only to MidKent College.

- Data released to parents, carers or guardians who are detailed on a student's records will normally be made without written consent of the student unless the student is aged over 18.

- Where students are aged between 18 and 25 and have an Education, Health and Care Plan (EHCP) or where they do not have the capacity to make their own decisions, parents/carers and guardians who are authorised to act on behalf of the student may have access to the student's data without the student's consent.

- If a student refuses or objects to the College sharing data with any or all of the parents, carers or guardians detailed on a student's records the College will:

    - consider the request on case by case basis but will apply a consistent approach in line with College procedures. When mitigating circumstances apply, the College reserves the right to depart from the College's procedures to ensure that the data subjects rights are administered transparently and to the best of the College's ability.
    - consider the request pursuant to Articles 18 and 19 of the UK GDPR (The Right to Restrict Processing) and pursuant to Article 21 of the UK GDPR (The Right to Object).
    - consider the request pursuant to the conditions being met under Schedule 1, (Special categories of Personal Data), Part 2, Substantial Public Interest Conditions, Paragraphs 16 and 18 of the Data Protection Act.
    - take into account that under data protection legislation, children and young adults can assume control over their personal information and restrict access to it in certain circumstances.

- For the purposes of parent/guardian requests, the College is not subject to the Education (Pupil Information) (England) Regulations 2005 as this only applies to any school maintained by a local education authority (other than a nursery school) and any special school not so maintained. The College is governed under legislation by the Further and Higher Education Act 1992. This Act removed colleges from local authority control and set them up as freestanding public bodies.

- The College also has a duty to comply with obligations set out in other legislation that give external organisation the power to act in loco parentis. This includes but is not limited to:

    - Care Act (2014) – this allows organisations to share data to promote individual wellbeing, support individual need for care and promote the integration of health and social care.
    - Children's Act (1989) – this allows organisations to share data to safeguard and promote the wellbeing of children.
    - Homelessness Reduction Act (2017) – this allows organisations to share data as part of taking reasonable steps to help applicants secure accommodation.
    - Keeping Children Safe in Education (Statutory guidance for schools and colleges) – this sets out the legal duties the College must follow to safeguard and promote the welfare of students under the age of 18.

- Employees must always follow internal procedures to determine whether they are permitted to share information with a parent, carer or guardian. If in any doubt, employees must seek advice from the Information Governance Team.

11.4 LAW ENFORCEMENT AGENCIES AND EMERGENCY SERVICES REQUESTS

- The College and the subsidiary company acknowledge that law enforcement agencies, in particular the police, have a key role to play in protecting the public whether that be; preventing or detecting a crime, apprehending offenders, protecting an individual's vital interest or following legal proceedings. However, the College and the subsidiary company recognises that law enforcement agencies, in particular the Police, do not have an automatic right to the personal data we hold on individuals and as such each request must be considered on its own merits and the appropriate legal basis applied when disclosing information. Before disclosing any personal data, the College and the subsidiary company must balance its priorities as an educational provider and its duties as a data controller, against its responsibilities to help protect the public and the community.

- The College and the subsidiary company aim to respond to all law enforcement agency and emergency services requests as quickly as possible, especially in circumstances covered under Emergency Information Requests (Vital Interest).

- In the event of any law enforcement request the College and the subsidiary company retains the right to contact the relevant authority to confirm the identity of the requesting officer.

11.4.1 EMERGENCY INFORMATION REQUESTS (VITAL INTERESTS)

- On the occasions that there is an emergency situation, pertaining only to matters of life and death, the lawful basis for processing of vital interests will

be invoked under Article 6(1)(d) of the UK GDPR. The College and the subsidiary company recognise that there is a high threshold required for this lawful basis to be applied - it must be essential to someone's life. Where possible the College and the subsidiary company will always seek to use an alternative lawful basis, for example legitimate interests, which provides a framework to balance the rights and interests of the data subject(s).

- Where vital interests arise in the context of health data, the College and the subsidiary company will consider the application of vital interests for special categories as a lawful basis for processing under Article 9(2)(a) of the UK GDPR. However, the College and the subsidiary company accepts this only applies if the data subject is physically or legally incapable of giving consent and that vital interests cannot be applied if the data subject refuses consent, unless they are not competent to do so. Where possible the College and the subsidiary company will always seek to use an alternative lawful basis, for example explicit consent.

11.4.2 NON-EMERGENCY INFORMATION REQUESTS

- In all other circumstances (outside of vital interests), the College and the subsidiary company will require the law enforcement agency to provide an Information Request Form. This requirement remains applicable in all non-life-situations regardless of the urgency. Where a request is urgent but not life threatening the College and the subsidiary company will aim to respond as quickly as possible whilst having due regard for the internal approval chain listed in the Law Enforcement Information Sharing Procedure.

- An Information Request Form is required regardless of whether the request is made in person, over the phone or via e-mail. The College and the subsidiary company retain the right to refuse a law enforcement request if an Information Sharing Form is not provided.

- Once the request has been received on the official form, it needs to be logged and approved internally before any information is released. This process is defined in the Law Enforcement Information Sharing Procedure.

- The College and the subsidiary company recognise that when a response is supplied in relation to an information request, it must do so in accordance with the seven principles set out under Article 5 of the UK GDPR.

12 ACCOUNTABILITY, ROLES AND RESPONSIBILITIES

12.1 DATA PROTECTION OFFICER (DPO)

- The DPO and the Information Governance Team is responsible for delivering the Information Governance Shared Service that covers both the College and the subsidiary company.

- The registered Data Protection Officer (DPO) acts for both the College and the subsidiary company.

- As prescribed under Article 39 of the UK GDPR, the following duties are within the responsibility and remit of the DPO:

    - Champion information governance requirements and issues across all levels of the College and the subsidiary company .
    - To inform and advise about the necessary obligations that should be undertaken to comply with data protection legislation and all other applicable laws. This includes delivering training on data protection legislation and all other applicable laws.
    - To advise and monitor compliance with data protection legislation and all other applicable laws, by conducting internal audits.
    - To advise and assist in the completion of data protection impact assessments (DPIA).
    - Continuously develop expertise on data protection sufficient to effectively fulfil the role.
    - Act as custodian(s) of the Retention Schedule and advise on the secure disposal of personal data.
    - To maintain current and accurate registration with the Information Commissioner's Office (ICO).
    - To be the first point of contact for the ICO and data subjects.
    - To be the initial contact for the investigation of data breaches and when and where required for reporting data breaches to the ICO.
    - Seek the advice of the ICO or lawyers where there is uncertainty around a data protection matter.
    - Carry out responses to requests made by data subjects in accordance with their rights.
    - Have due regard to the risk associated with processing operations, considering the nature, scope, context and purposes of processing when approving processing activities and data protection impact assessments.
    - Maintain the Records of Processing Activities as required by Article 30 of the UK GDPR to document regular processing activities.

- In accordance with the above, the DPO is authorised to request and access any information that falls within scope of their responsibilities.

12.2 INFORMATION GOVERNANCE GROUPS

- The College and the subsidiary company designate responsibility to overseeing the implementation of Information Governance to the respective Information Governance Groups.

- The duties, responsibility and remit of the Information Governance Groups are detailed in their respective Terms of Reference.

- The Information Governance Groups are chaired by the DPO.

12.3 INFORMATION GOVERNANCE TEAM (SHARED SERVICE)

- The College and the subsidiary company designate responsibility to for implementing the decision of Information Governance Groups.

- The Information Governance Teams is responsible for investigating data breaches, responding to data subject rights requests, assisting with the completion of Records of Processing Activities, data protection impact assessment and privacy notices, and supporting the delivery of data protection compliance,

- The Information Governance Team is managed by the DPO.

12.4 GOVERNING BODY AND BOARD OF DIRECTORS

- The following duties are within the responsibility and remit of the Governing Body at the College and the Board of Directors for the subsidiary company:

    - Promote data protection and model best practice.
    - Maintain oversight of data protection across to ensure compliance with legislation.
    - Pursuant to Article 38 (2) of the UK GDPR, ensure that adequate resources are available for the implementation of data protection policies and procedures.
    - Ensure that data protection is integrated into policies and procedures as and when they relate to personal data.
    - Foster an environment in which employees are not put under any undue influence or pressure to breach this policy.

12.5 EXECUTIVE DIRECTORS

- The following duties are within the responsibility and remit of the Executive Directors:

    - Promote data protection and model best practice.
    - Delegate responsible for implementing data protection to the Information Governance Groups.
    - Maintain oversight of data protection across to ensure compliance with legislation.
    - Appoint a Data Protection Officer as per the reasons listed in Article 37 of the UK GDPR.
    - Pursuant to Article 38 (2) of the UK GDPR, ensure that adequate resources are available for the implementation of data protection policies and procedures.
    - Pursuant to Article 38 (2, 3, 6) of the UK GDPR, ensure that the role of the Data Protection Officer remains independent and free from bias and conflict(s) of interest.

- Pursuant to Article 38 (3) of the UK GDPR, which states *"…The Data Protection Officer shall directly report to the highest management level of the controller or the processor..."*, ensure that the position of the DPO will be held by, or report to, a member of the Executive Team.
- Pursuant to Article 38 (1) of the UK GDPR, *"…ensure that the Data Protection Officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data."*
- Pursuant to Article 37 (5) of the UK GDPR ensure that *"The Data Protection Officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39."*
- Ensure that data protection is integrated into policies and procedures as and when they relate to personal data.
- Foster an environment in which employees are not put under any undue influence or pressure to breach this policy.

12.6 SENIOR LEADERSHIP TEAM AND COLLEGE LEADERSHIP TEAM

- The following duties align with the responsibilities and remit of managers who form the College Leadership Team and Senior Leadership Team:

    - Developing and encouraging data protection best practices.
    - Maintaining oversight of data protection within their respective departments/service areas to ensure compliance with legislation in day to day activities.
    - Working with the DPO to ensure any necessary compliance measures identified are implemented within their respective departments/service. Such compliance measures may arise from, but are not limited to, data protection impact assessments (DPIA), employee training, audits, data breaches.
    - To assist the Information Governance Team with requests pertinent to data protection including, but not limited to, data breaches and requests made under section 8 Data Subject Rights.

12.7 SENIOR MANAGER RESPONSIBLE FOR ICT

- The following duties align with the responsibilities and remit of the above post-holder:

    - To ensure that appropriate and adequate technical measures are in place to safeguard the security of data.
    - To advise and recommend additional requirements and developments that can be implemented to enhance the security of the data and processes.
    - To maintain awareness and understanding of current cybersecurity thefts.

12.8 SENIOR MANAGER RESPONSIBLE FOR HUMAN RESOURCES (HR)

- The following duties align with the responsibilities and remit of the above post-holder:

    - To maintain oversight of personal data processed with regards to employees, that relates to the functions carried out by Human Resources.
    - To work with the DPO to ensure the security and integrity of the personal data processed with regards to employees, that relates to the functions carried out by Human Resources.
    - To work with the DPO to ensure that the College and the subsidiary company responds to changes in legislation that will impact employees' personal data.
    - To ensure that the College and the subsidiary company provides a mechanism for employees to complete mandatory data protection training on a regular basis.

12.9 SENIOR MANAGER RESPONSIBLE FOR MANAGEMENT INFORMATION SYSTEMS (MIS)

- The following duties align with the responsibilities and remit of the above post-holder:

    - To maintain oversight of personal data processed with regards to students. This includes admissions, examinations and academic performance data.
    - To work with the DPO to ensure the security and integrity of students' personal data processed within the MIS system(s).
    - To work with the DPO to ensure that the College and the subsidiary company responds to changes in legislation that will impact employees' personal data.

12.10 EMPLOYEES AND INDIVIDUALS WORKING ON BEHALF OF THE COLLEGE AND SUBSIDARY COMPANY

- All employees and individuals working on behalf of the College and the subsidiary company are expected to:

    - familiarise themselves with the Privacy Notices provided.
    - familiarise themselves and work in accordance with this policy and the Information Charter. It should be noted that all users agree to these policies when signing into their College account.
    - ensure that their personal details provided for employment purposes is accurate and up to date.
    - not respond to requests made in relation to data subjects' rights, but instead to refer the request to the Information Governance Team.

- ensure that any personal data for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised.
- only use College approved devices (as per the College's ICT Policies) for work unless there are mitigating circumstances. For example, within the subsidiary company, using a client ICT system where necessary to fulfil contractual obligations.
- not bring unauthorised data including, but not limited to, personal data not required for employment purposes, data that is not relevant to completing the job role or data that is not related to the operational requirements, into the building or onto the College's network.
- complete all required mandatory data protection training.
- only keep personal data in accordance with the Retention Schedule.
- take care when connecting to public wi-fi to complete work, as these can expose your connection to interception. If in doubt do not connect to it.
- take care to e-mail the intended recipient, especially when using autocomplete, and use the 'bcc' field when emailing multiple people.
- report any suspected or confirmed personal data breaches to the Information Governance Team as soon as possible.
- seek advice from the Information Governance Team where there is uncertainty around a data protection matter.

12.11 STUDENTS AND LEARNERS

- MidKent College Students are responsible for:

    - familiarising themselves with the Privacy Notice.
    - familiarise themselves with the contents of this policy and ICT Policies, in particular the Acceptable Use Agreement. It should be noted that all users agree to these policies when signing into their College account.
    - ensuring that their personal data provided is accurate and up to date.
    - treating people's personal information with integrity and confidentiality and not to hand out personal details just because someone asks.
    - not bring unauthorised data including but not limited to personal data not required for learning purposes onto the College's network.
    - take care when connecting to public wi-fi to complete work, as these can expose your connection to interception. If in doubt do not connect to it.
    - take care to e-mail the intended recipient, especially when using autocomplete, and use the 'bcc' field when emailing multiple people.
    - report any suspected or confirmed personal data breaches to a member of staff as soon as possible.

13 DATA PROTECTION BY DESIGN AND DEFAULT

- The College and the subsidiary company are committed to complying with Articles 25(1) and 25(2) of the UK GDPR, which outline obligations concerning data protection by design and by default.

- The College and the subsidiary company recognise that it has an obligation to take pro-active steps to consider the impact on data privacy during all processing activities. This includes implementing appropriate technical and organisational measures to minimise the potential negative impact processing can have on the data subjects' privacy and only processing data that is necessary to achieve the specified purpose.

- When considering processing activities, the College and the subsidiary company will assess the risks that these may pose to individuals, and the possible measures available to ensure compliance with the data protection principles and protect individual rights. These considerations must cover:

    - the state of the art and costs of implementation of any measures;
    - the nature, scope, context and purposes of your processing; and
    - the risks that your processing poses to the rights and freedoms of individuals.

- To demonstrate commitment to data protection by design and default, where possible, the College and the subsidiary company will always endeavour to:

    - design/purchase any system, service, product, and/or business practice that has privacy settings built in to protect personal data automatically.
    - embed data protection into the design of any systems, services, products and business practices.
    - use systems, services, products and business practices that cater to both adequate privacy and security obligations.
    - put in place strong security measures from the beginning of a project and extend this security throughout the life of the project.
    - ensure that all systems, services, products and business practices operate in accordance with the reason the data was collected.
    - respect user's privacy.

13.1 RECORDS MANAGEMENT

- The College and the subsidiary company recognise that robust records management is integral to information security and is committed to implementing procedures to reflect this in order to ensure compliance with the data protection legislation.

- The College and the subsidiary company endeavours to integrate records management procedures that record: the date of creation, version control, document classification, access permissions, retention period and destruction date into all operational activities.

- The College and the subsidiary company will provide or facilitate arrangements for a secure facility to store paperwork that meets the identified archiving requirements.

13.2 DATA PROTECTION IMPACT ASSESSMENT

- When the College and/or subsidiary company considers carrying out new or amended processing activities that involve personal data, privacy issues must always be assessed and a Data Protection Impact Assessment (DPIA) must be conducted.

- The College and the subsidiary company will ensure that all completed DPIA's meet:

    - the recommendations listed in the European Data Protection Board 'Guidelines on Data Protection Impact Assessment';
    - the requirements of Articles 35 and 36 of the UK GDPR; and
    - the guidance issued by the ICO.

14 DATA BREACHES

- A breach of data is defined as a security incident that has adversely affected the confidentiality, integrity or availability of personal data. This could include:

    - hacking or other forms of unauthorised access by a third party;
    - deliberate or accidental action (or inaction) by a controller or processor;
    - sending personal data to an incorrect recipient;
    - loss or theft of devices or data;
    - alteration of personal data without permission; and
    - loss of availability of personal data.

- Where an employee discovers or suspects a personal data breach, this should be reported to the Information Governance Team as soon as possible.

- Where a data breach is identified as part of a disciplinary investigation the Data Protection Officer will be notified and agree with Human Resources to manage and respond to the incident on a case by case basis, taking into account the sensitivities of the situation.

- The College and the subsidiary company acknowledge that data breaches can happen at any time and as such will ensure measures are in place to respond to breaches regardless of the date and time they occur.

- Where there is a likely risk to individuals' rights and freedoms, the Data Protection Officer will report the personal data breach to the ICO within 72 hours of the organisation being aware of the breach.

- The College and the subsidiary company acknowledge that failure to notify the ICO about a breach could result in significant penalties of either a maximum fine of £17.5 million or 4% of annual turnover, whichever is greater. In addition, significant breaches are also likely to result in damage to the College's and the subsidiary company 's reputation.

- Where there is also a likely high risk to individuals' rights and freedoms, the College and the subsidiary company will inform those individuals without undue delay; unless subsequent steps have been taken to ensure that the risk is unlikely to materialise, security measures were applied to render the personal data unintelligible (this includes but is not limited to encryption), or it would amount to disproportionate effort to inform the data subject directly. In the latter circumstances, a public communication must be made, or an equally effective alternative measure must be adopted to inform data subjects, so that they themselves can take any remedial action.

- The Information Governance Team will keep a record of all personal data breaches reported and follow up with appropriate measures and improvements to reduce the risk of reoccurrence.

- Any students found to have acted in a manner that compromises this policy, especially where the action was deliberate, will be dealt with under Student Disciplinary Policy. In cases where a breach is also deemed to be a criminal offence, the matter will be reported as soon as possible to the appropriate authorities.

- Any employees found to have acted in a manner that compromises this policy, especially where the action was deliberate, will be dealt with under Staff Disciplinary Policy. In cases where a breach is also deemed to be a criminal offence, the matter will be reported as soon as possible to the appropriate authorities.

- Offences which are considered to be gross misconduct include but are not limited to:

    - Deliberate unlawful disclosure of personal data.
    - Inappropriate use of personal data.
    - Deliberately accessing special category personal data in the absence of a legitimate business reason for doing so.
    - Misuse of personal data which results in a claim being made against the College and/or the subsidiary company.

        - This does not affect an employee's right to whistle blow or to freedom of speech, but rather to run in parallel with policies on these matters.

- Failure to provide information requested as part of a data breach investigation is also considered to be a breach of this policy and will be dealt with under Staff Disciplinary Policy.

15 POLICY MONITORING, REVIEW AND EVALUATION

- A review of this policy will be undertaken by the review date by the policy writer and the Senior Manager responsible. The policy will then be presented to Risk and Audit Committee, the Board of Directors of the subsidiary company and the Full Governing Body for approval.

16 EQUALITY IMPACT ASSESSMENT

- This policy has been Equality Impact Assessed and generates no concerns about differential impact. The Equality Impact Assessment is filed on the Quality SharePoint site.

17 POLICY DISTRIBUTION

- A current version of this document is available via SharePoint and on the College website. It does not contain confidential information and can be released to external parties.