General Data Protection Policy

Once printed, this document is uncontrolled. Please refer to the current version on KC Share.

Document Owner	Head of IT and Digital Vision
Title of Document	General Data Protection Policy
Status	Approved
Reviewed By	Information Assurance Group
Approved by	Corporation – 22 May 2023
Collective Agreement?	No
Shared with Unions for comments:	UCU: ~~yes~~/no Unison: ~~yes~~/no NEU: ~~yes~~/no
Publication Date	June 2023
Review Date	Within two years of last approval date
Distribution	KC Share/website
Reason for Update/Creation	Scheduled periodic review; Updating
Related Policies/ Procedures	Staff Code of Conduct Disciplinary Policy & Procedure Acceptable Use Policy Data Retention Policy Data Breach Notification Procedure Rights of Individuals Policy Rights of Individuals Procedure Major Incident & Business Continuity Plan

TABLE OF CONTENTS

1. INTRODUCTION AND PURPOSE

1.1. The purpose of this General Data Protection Policy ("Policy") is to ensure all College Personnel understand the legal and regulatory framework for data protection and how to contribute to safe working practices.

1.2. College Personnel will receive a copy of this Policy as part of their induction and may receive periodic revisions. This Policy does not form part of any contract of employment and the College reserves the right to change it at any time.

1.3. If you have queries about this Policy, please contact our Data Protection Officer, who is responsible for ensuring compliance with this Policy.

2. OUR VALUES AND BEHAVIOURS

2.1. Our College values and behaviours helped us shape this Policy. Our values inspire our everyday work; students, staff and governors all had a voice in shaping them and we are proud of what we came up with together: Kindness, Unity and Excellence.

3. SCOPE

3.1 This Policy applies to:

- All members of the College community and others who process College information and/or work in locations where information is stored (staff, agency staff, students, governors, other volunteers, contractors, etc.);
- All College information assets, except for information that would cause no impact if it was compromised or lost, such as information in or intended for the public domain.

4. DEFINITIONS

4.1. **Automated Decision Making** - Where a decision about an Individual is made solely by automated means without any human involvement and the decision has legal or other significant effects.

4.2. **College** – Kirklees College

4.3. **College Personnel** – Any College employee, worker or contractor, including employees, consultants, contractors, governors and temporary personnel working on behalf of the College.

4.4. **Controller** – Any entity (e.g. company, organisation or person) that makes its own decisions about how it is going to collect and use Personal Data.

A Controller is responsible for compliance with Data Protection Laws. The College will be the 'Controller' of Personal Data if it decides what Personal Data it is going to collect and how it will use it. A common misconception is that individuals within organisations are the Controllers. This is not the case; it is the organisation itself which is the Controller.

4.5. **Data Protection Laws** – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of Section 3 of the European Union (Withdrawal) Act 2018 and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator, including the Data Protection Act 2018 as amended.

4.6. **Data Protection Officer –** Our Director of Governance & Compliance Ms J Green, who may be contacted at: 07738 973114 gdpr@kirkleescollege.ac.uk.

4.7. **EEA** – Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden.

4.8. **ICO** – the Information Commissioner's Office, the UK's data protection regulator.

4.9. **Individuals** – Living individuals who can be identified, *directly or indirectly*, from information that the College has. For example, an individual could be identified directly by name, or indirectly by sex, job role and office location if this information could be used to work out who they are. Individuals include employees, students, parents, visitors and potential students. Individuals also include partnerships and sole traders.

4.10. **Personal Data** – Any information about an Individual (see definition above) which identifies them or allows them to be identified in conjunction with other information that is held. It includes information of this type, even if used in a business context. 'Personal Data' is defined broadly and covers things such as name, address, email address (including in a business context, email addresses of Individuals such as firstname.surname@organisation.com), IP address and also more sensitive types of data such as trade union membership, genetic data and religious beliefs. These more sensitive types of data are called "Special Categories of Personal Data" and are defined below. Special Categories of Personal Data are given extra protection by Data Protection Laws.

4.11. **Processor** – Any entity (e.g. company, organisation or person) which accesses or uses Personal Data on the instruction of a Controller.
A Processor is a third party that processes Personal Data on behalf of a Controller. This is usually as a result of the outsourcing of a service by the Controller or the provision of services by the Processor which involve access to or use of Personal Data. Examples include: where software support for a system which contains Personal Data is provided by someone outside the business; cloud arrangements; and mail fulfilment services.

4.12. **Profiling** – Happens where the College automatically uses Personal Data to evaluate certain things about an Individual.

4.13. **Special Categories of Personal Data** – Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.

5. COLLEGE PERSONNEL'S GENERAL OBLIGATIONS

5.1. All College Personnel must comply with this Policy. In particular, College Personnel must ensure that they keep confidential all Personal Data that they collect, store, use and come into contact with during the performance of their duties.

5.2. College Personnel must not release or disclose any Personal Data:

5.2.1. outside the College; or

5.2.2. inside the College to College Personnel not authorised to access the Personal Data

without specific authorisation from their manager or the Data Protection Officer.

5.3. College Personnel must take all steps to protect College information assets from damage, theft and unauthorised access - whether by other College Personnel who are not authorised to have access, or by people outside the College. This includes closing and locking doors and windows, making use of secure storage, following procedures for disposal and transfer, setting alarms,and ensuring security lighting and CCTV is activated as necessary.

6. THE DATA PROTECTION PRINCIPLES

6.1. When using Personal Data, Data Protection Laws require that the College complies with the following principles. Personal Data must be:

6.1.1. processed lawfully, fairly and in a transparent manner;

6.1.2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

6.1.3. adequate, relevant and limited to what is necessary for the purposes for which it is being processed;

6.1.4. accurate and kept up to date, meaning that every reasonable step must be taken to ensure that Personal Data that is inaccurate is erased or rectified as soon as possible;

6.1.5. kept for no longer than is necessary for the purposes for which it is being processed; and

6.1.6. processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

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

6.3. In addition to complying with the above requirements the College also has to demonstrate in writing that it complies with them. The College has a number of policies and procedures in place, including this Policy and the documentation referred to in it, to ensure that the College can demonstrate its compliance.

7. LAWFUL USE OF PERSONAL DATA

7.1. In order to collect and/or use Personal Data lawfully, the College needs to be able to show that its use meets one of a number of legal grounds. Please click here for detailed information about the lawful bases for processing: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing

7.2. In addition, when the College collects and/or uses Special Categories of Personal Data, the College has to show that one of a number of additional conditions is met. Please click here to see the detailed additional conditions https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/#scd3.

7.3. The College has carefully assessed how it uses Personal Data and how it complies with the obligations set out in paragraphs 7.1 and 7.2. If the College changes how it uses Personal Data, the College needs to update this record and may also need to notify Individuals about the change.

8. TRANSPARENT PROCESSING – PRIVACY NOTICES

8.1. Where the College collects Personal Data directly from Individuals, the College will inform them about how the College uses their Personal Data. This is in a privacy notice. Links to the College's privacy notices are below:

Student Privacy Notice
Applicant Privacy Notice
Staff Privacy Notice
Third Party (non-student and staff) Privacy Notice

8.2. If the College receives Personal Data about an Individual from other sources, the College will provide the Individual with a privacy notice explaining how the College will use their Personal Data. This will be provided as soon as reasonably possible and in any event within one month.

8.3. If the College changes how it uses Personal Data, the College may need to notify Individuals about the change. College Personnel intending to introduce a new process involving Personal Data, or to change the way Personal Data is used, should notify the Data Protection Officer who will decide whether the intended use requires amendments to be made to the privacy notices and any other controls which need to apply.

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

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

9.2. All College Personnel that collect and record Personal Data shall ensure that the Personal Data is recorded accurately, is kept up to date and shall also ensure that they limit the collection and recording of Personal Data to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used.

9.3. All College Personnel that obtain Personal Data from sources outside the College shall take reasonable steps to ensure that the Personal Data is recorded accurately, is up to date and limited to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. This does not require College Personnel to independently check the Personal Data obtained.

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

9.5. The College recognises the importance of ensuring that Personal Data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection Laws. The College has a Rights of Individuals Policy and a Rights of Individuals Procedure which set out how the College responds to requests relating to these issues. Any request from an Individual for the amendment, rectification, erasure or restriction of the use of their Personal Data should be dealt with in accordance with those documents.

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

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

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

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

11. DATA SECURITY

11.1. The College takes information security very seriously and the College has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. The College has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

12. DATA BREACHES

12.1. We operate in an environment where cyber-crime is on the rise, technology is advancing at a phenomenal rate and businesses are processing an unprecedented volume of data. It is almost inevitable that large organisations will experience some data breaches and possibly this will result in the unauthorised loss of, access to, deletion of or alteration of Personal Data. If and when this happens, College Personnel must comply with the College's Data Breach Notification Policy. Please see paragraphs 12.2 and 12.3 below for examples of what can be a Personal Data breach. All College Personnel should be familiar with the Data Breach Notification Policy, as it contains important obligations which must be complied with in the event of Personal Data breaches, including details of the information to be provided when reporting a breach.

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

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

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

12.3.2. **Availability breach** - where there is an accidental or unauthorised loss of access to, or destruction of, Personal Data e.g. loss of a memory stick, laptop or device, denial of service attack, infection of

systems by ransom ware, deleting Personal Data in error, loss of access to Personal Data stored on systems, inability to restore access to Personal Data from back up, or loss of an encryption key; and

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

12.4. In some cases, a data breach may amount to, or form part of, a 'Major Incident', involving significant disruption to a level which potentially overwhelms normal activities and procedures. In such cases, a member of the College Executive Team may implement the Major Incident & Business Continuity Plan.

13. APPOINTING CONTRACTORS WHO WILL ACCESS COLLEGE PERSONAL DATA

13.1. Before the College appoints a contractor to be a Processor of College Personal Data, Data Protection Laws require it to carry out due diligence and put appropriate contractual agreements in place. The Data Protection Officer can help with the negotiation and drafting of data processing and information sharing agreements. Contact GDPR@kirkleescollege.ac.uk.

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

13.3. Any contract where a Controller appoints a Processor must be in writing.

13.4. A Controller is deemed to have appointed a Processor when it engages someone to perform a service for it and as part of it they may get access to the Controller's Personal Data. A Controller that appoints a Processor remains responsible for what happens to the Personal Data.

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

13.5.1. to only act on the written instructions of the Controller;

13.5.2. to not export Personal Data without the Controller's instruction;

13.5.3. to ensure staff are subject to confidentiality obligations;

13.5.4. to take appropriate security measures;

13.5.5. to only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;

13.5.6. to keep the Personal Data secure and assist the Controller to do so;

13.5.7. to assist with the notification of Data Breaches and Data Protection Impact Assessments;

13.5.8. to assist with data subject requests, such as access, rectification, right to restrict processing, right to be forgotten;

13.5.9. to delete/return all Personal Data as requested at the end of the contract;

13.5.10. to submit to audits and provide information about the processing; and

13.5.11. to tell the Controller if any instruction is in breach of the Data Protection Laws.

13.6. In addition, the contract should set out:

13.6.1. The subject-matter and duration of the processing;

13.6.2. the nature and purpose of the processing;

13.6.3. the type of Personal Data and categories of Individuals; and

13.6.4. the obligations and rights of the Controller.

13.7. The College maintains a record of all processing activities carried out by any Processors on its behalf. Any manager who appoints a Processor must notify the Data Protection Officer and provide them with a copy of the contract, prior to the commencement of any processing activity.

14. INDIVIDUALS' RIGHTS

14.1. The College's Rights of Individuals Policy describes the rights of Individuals in respect of their personal data. Briefly, these are:

Subject Access Requests - the right to ask any Controller to confirm what Personal Data is held in relation to them and to provide them with the data;

The Right of Erasure/to be Forgotten - the right of an Individual to request the erasure of their Personal Data in certain circumstances;

The Right of Data Portability – the right of an Individual to request that their Personal Data is provided to them in a structured, commonly used and machine-readable format where:

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

The Right of Rectification and Restriction – the right to request that any Personal Data is rectified if inaccurate and to have use of Personal Data restricted to particular purposes in certain circumstances.

14.2. The College will use all Personal Data in accordance with the rights given to Individuals' under Data Protection Laws, and will ensure that it allows Individuals to exercise their rights in accordance with the College's Rights of Individuals Policy and Rights of Individuals Procedure. These documents contain important obligations which College Personnel must comply with.

15. MARKETING AND CONSENT

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

15.2. **Marketing** consists of any advertising or marketing communication that is directed to particular Individuals. Where marketing activity is contemplated, this must be identified in relevant privacy notices, and must include detailed information, such as whether any profiling takes place. There are strict rules on obtaining consent requiring an Individual's "clear affirmative action". The ICO prefers to see the 'consent' basis used in a marketing context.

15.3. The Privacy and Electronic Communications Regulations (PECR) apply to direct marketing i.e. a communication directed to particular Individuals and cover any advertising/marketing material. They apply to electronic communication i.e. calls, emails, texts, faxes. The PECR apply even if the College is not processing any Personal Data.

15.4. Consent is central to electronic marketing. The College will normally seek consent (where appropriate) by providing an un-ticked opt-in box.

15.5. Alternatively, the College may be able to market using a "soft opt in" if the following conditions are met:

15.5.1. contact details have been obtained in the course of a sale (or negotiations for a sale);

15.5.2. the College is marketing its own similar services; and

15.5.3. the College gives the Individual a simple opportunity to refuse to opt out of the marketing, both when first collecting the details and in every message after that.

16. AUTOMATED DECISION MAKING AND PROFILING

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

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

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

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

17. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

17.1. A Data Protection Impact Assessment (**"DPIA"**) must be completed where the use of Personal Data is likely to result in a high risk to the rights and freedoms of Individuals. A DPIA should be started as early as practical in the design of processing operations. A DPIA is not a prohibition on using Personal Data but is an assessment of issues affecting Personal Data which need to be considered before processing begins. The process is designed to:

17.1.1. describe the collection and use of Personal Data;

17.1.2. assess its necessity and its proportionality in relation to the purposes;

17.1.3. assess the risks to the rights and freedoms of Individuals; and

17.1.4. the measures to address the risks.

17.2. Where a DPIA reveals risks which cannot be appropriately mitigated, the ICO must be consulted.

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

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

17.4.1. large scale and systematic use of Personal Data for the purposes of Automated Decision Making or Profiling (see definitions above) where legal or similarly significant decisions are made;

17.4.2. large scale use of Special Categories of Personal Data, or Personal Data relating to criminal convictions and offences e.g. the use of high volumes of health data; or

17.4.3. systematic monitoring of public areas on a large scale e.g. CCTV cameras.

17.5. All DPIAs must be reviewed and approved by the Data Protection Officer. Contact the Data Protection Officer for advice and support with Data Processing Impact Assessments.

17.6. There is advice on when and how to carry out a Data Processing Impact Assessment on the Information Commissioner's website and the College has a software system called GDPR Sentry which explains the process step by step.

18. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE UK

18.1. Data Protection Laws impose strict controls on the transfer of Personal Data outside the UK. Transfer includes sending Personal Data outside the UK but also includes storage of, or access to, Personal Data outside the UK.

18.2. UK Controllers can continue to make transfers of data from the UK to the EEA under UK adequacy regulations but appropriate transfer mechanisms must be considered whenever the College appoints a supplier outside the UK and the EEA or the College appoints a supplier with group companies outside the UK and the EEA which may give access to the Personal Data to staff outside the UK and the EEA.

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

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

19. REVIEW OF POLICY

19.1. Comments, questions and feedback on this Policy are welcome via the itservicedesk@kirkleescollege.ac.uk.

19.2. The Executive Director of Business Systems shall have authority to make changes to this Policy to reflect changes to personnel or job roles, contact details, typographical errors or changes to legislation or related policies referenced within it. Any material changes must be approved by the Corporation.