

Data Protection Policy/GDPR

**This Policy includes:**

Data Protection and GDPR

Records Management

Records and Data retention Schedule



**Data Protection Act 2018 and GDPR \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Introduction**

On the 25th May 2018 the General Data Protection Regulation (EU 2016/679) replaced the EU Data Protection Directive, this superseded the laws of individual EU member states and required these states to replace their own directives around Data Protection this led to the UK bringing into place the Data Protection Act 2018.

The purpose of both DPA 2018 and GDPR is to protect the rights and freedoms of living individuals, to ensure that their data is not processed without their knowledge, and wherever possible that it is processed with their consent.

**Scope and Rationale**

CANTO Learning Ltd needs to gather and use certain information about individuals in certain cases data will be held to meet legal obligations held towards our stakeholders.

CANTO Learning Ltd needs to process certain information about its staff, students, parents and guardians and other individuals with whom it has a relationship for various purposes such as, but not limited to:

1. The recruitment and payment of staff.
2. The administration of programmes of study and courses.
3. Student enrolment.
4. Examinations and external accreditation.
5. Recording student progress, attendance and conduct.
6. Collecting payments.
7. Complying with legal obligations to funding bodies and government including local government.

To ensure we comply with the various legal obligations, including the obligations imposed on it by the General Data Protection Regulation (GDPR) CANTO Learning Ltd must ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

The primary purpose of the data protection policy is to ensure that CANTO Learning Ltd:

* Complies with data protection law and follows good practice.
* Protects the rights of students, staff and partners.
* Is open about how it stores and processes individuals’ data.
* Protects itself from the risk of a data breach.

CANTO Learning’s compliance with the Data Protection Law is covered by this policy and other policies such as: Data Retention Schedule, IT Security Policy, Privacy Policy, Cookies Policy.

It is the policy of the College to ensure that all members are aware of the requirements of data protection legislation in relation to their individual responsibilities.

**Compliance**

This policy applies to all staff and students of CANTO Learning Ltd. Any breach of this policy or of the Regulation itself will be considered an offence and the College’s disciplinary procedures will be invoked.

As a matter of best practice, other agencies and individuals working with CANTO Learning Ltd who have access to personal information, will be expected to read and comply with this policy. It is expected that staff who are responsible for dealing with external bodies will take the responsibility for ensuring that such bodies comply with our data protection policy.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR/DPA 2018 and other relevant legislation.

**Responsibilities under the GDPR**

CANTO Learning Ltd will be the ‘data controller’ under the terms of the legislation – this means it is ultimately responsible for controlling the use and processing of the personal data. The college has a member of the Senior Leadership Team who is responsible for overseeing data protection processes, the college also has a trustee who has been nominated to oversee this policy.

The Senior Management Team is responsible for all day-to-day data protection matters, and will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling within the college.

The Senior Leadership Team is also responsible for ensuring that the college’s notification is kept accurate. Details of the College’s notification can be found on the Office of the Information Commissioner’s website. Our data registration number is ZA367984.

Compliance with the legislation is the personal responsibility of all members of staff at the College who process personal information, have access to or knowledge of personal information.

All staff members should be aware of the guidelines of DPA 2018/GDPR and work to ensure they do not disclose any information to an unauthorised person or source.

Staff are also responsible for ensuring that their passwords are appropriate and that these are not shared with others placing risk on their devices or accounts.

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

CANTO Learning Ltd will take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data. Filing systems and the preservation of secure passwords for access to relevant data held on computer should be strictly observed.

Personal data about an individual must not be placed on the world wide web unless the individual whose data is used has given his or her express consent.

Any data protection concerns should be addressed to the senior leadership team in the first instance.

**Processing Personal Data**

**What constitutes personal data?**Any information related to a natural person or ‘Data Subject’, that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

Under GDPR Law CANTO Learning Ltd is obliged to ensure that all data shall:

1. **Be processed fairly and lawfully;**
2. **Be held only for specified purposes and not used or disclosed in any way incompatible with those purposes;**
3. **Be adequate, relevant and not excessive;**
4. **Be accurate and kept up-to-date;**
5. **Not be kept for longer than necessary for the particular purpose;**
6. **Be processed in accordance with data subjects’ rights;**
7. **Be kept secure;**
8. **Not be transferred outside the European Economic Area unless the recipient country ensures an adequate level of protection.**

These rules apply whether data is stored electronically, on paper or on other materials.  To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.  Processing of data includes any activity that involves the handling of data including its, collection, use, storage, adaption, dissemination or disposal.

In view of the recent global pandemic it should be recognised that although medical information is considered sensitive, under GDPR article 9 there is provision for this information to be shared without consent should it be deemed of public interest.  However consideration will always be given to data  security and this will be applied on an individual case basis. Under this guidance CANTO has the right to request information regarding travel and socialisation to safeguard the college community

Any processing of such information must be done in accordance with the principles outlined above. To comply with the first principle (fair and lawful processing), at least one of the following conditions must be met:

 **The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:**

**(a) Consent:**the individual has given clear consent for you to process their personal data for a specific purpose.

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

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

**(d) Vital interests:**the processing is necessary to protect someone’s life.

**(e) Public task:**the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

**(f) Legitimate interests:**the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

In all instances where consent is needed this will be requested in an easily accessible form, with the purpose for data processing attached to that consent - meaning it must be unambiguous. Consent must be clear, using clear and plain language. It must be as easy to withdraw consent as it is to give it.​  Explicit consent is required only for processing sensitive personal data - in this context, nothing short of “opt in” will suffice. However, for non-sensitive data, “unambiguous” consent will suffice see *Article 7 and in Recital 42 where the GDPR states that “where processing is based on the data subject’s consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation.”)*.

**Data Security**

CANTO Learning Ltd takes the data security seriously and to reduce the risk of a data breach and has undertaken several technical measures.  This includes email and other forms of encryption.  Our 3rd party IT company support CANTO in this process maintaining and monitoring our server and cloud for possible breaches.  Data stored on paper will be held within locked rooms and shredded when no longer needed. Privacy Impact Assessments will monitor along with regular checks on data by the quality assurance team.  Staff are kept informed of CANTO’s data protection policy and training is provided when appropriate.

All staff are aware that appropriate permissions are needed for personal data and that this must be kept securely at all times whether in paper or electronic format.

No personal data should be passed on orally to an unauthorised third party without the express consent of the data subject.

 **Bring your own device**

To ensure that CANTO fully meets both Data Protection Policy/GDPR and appropriate IT security guidance we currently request that all work related tasks take place on an organisation owned device whether this be laptop, smart phone or tablet when working on tasks that contain individuals data/image.

**Photographs within the college**

To ensure that CANTO meets high standards for data protection it will request specific consent when using individual’s pictures for varying data processing reasons.  Due to the variety of processing reasons these need to be considered separately and some are outlined below, it should be noted that these are not exclusive to the college but in all cases specific consent will be requested and clear guidelines given as to the use and length of time these will be maintained for.

**Photographs within the college**

Photographs used in the identity management can be essential as part of an individuals programme, however once an individual leaves the college this should be deleted as it is no longer needed for the purpose for which it was held.

Photographs used in displays within the building will require consent from the individual for this purpose, on giving consent it will be agreed that no picture will be displayed for longer than 6 months.  Once the individual leaves the college pictures on display will be removed unless additional consent has been obtained.  This additional consent maybe particularly relevant should this picture form part of a larger display.  If additional consent is sort this should be for no longer than an additional period of 6 months.

Photographs to be used on the website/facebook or other social media platforms must have explicit consent from the individual for a period of 12 months.  Regular checks are to take place of these sites to ensure that appropriate consent is obtained for all individuals featuring.  When a student leaves additional consent may be obtained to allow a particular picture or pictures to feature, the consent in this case must be specific and monitored.

Photographs to be used in promotional material will have explicit consent from the individual.

This consent will state that images will be maintained on the promotional material for a period of up to 12 months. Regular checks are to take place of the material to ensure that appropriate consent is obtained for all individuals featuring.  When a student leaves additional consent may be obtained to allow particular picture to feature, consent in this case must be specific and monitored.

Photographs to be used in promotional material such as banners etc will have explicit consent from the individual.  Due to costs involved in the creation of such promotional materials it is recognised for this that these materials would need to be kept for a longer period of time.  When seeking consent from individuals for this purpose clear guidance will be given as to the use and the length of time the consent is required for before permission is requested.

**Privacy by design**

CANTO Learning Ltd undertakes an approach to activities within the organisation that incorporates privacy and data protection compliance from the start. To comply with Article 25 of GDPR the college ensures that appropriate organisational and technical measures are in place to support the handling of data. To ensure that privacy by design is embedded within the organisation Data Privacy Impact Assessments are implemented to support this process.

**Data Privacy Impact Assessments (DPIA’s)**

To ensure that CANTO complies with Article 35 DPIA’s will be carried out when it is assessed that a processing activity may take place that could place a high risk on data.  As part of this the college will ensure that the DPIA is in place early in the life of a new processing activity so that risks can be assessed and recommendations made and implemented. A CANTO Learning DPIA will seek to

* 1. Identify the need for a DPIA.
* 2. Describe the information flow.
* 3. Identify data protection and related risks.
* 4. Identify data protection solutions to reduce or eliminate the risks.
* 5. Sign off the outcomes of the DPIA.
* 6. Integrate data protection solutions into the processing activity.

**Right to be forgotten/Right to erasure**

Under Article 17 of GDPR individuals have a right to have personal data erased.  This is also known as the ‘right to be forgotten’ and is newly implemented.  The right only is not absolute and only applies in certain circumstances.

The college will apply the right to erasure if:

* The personal data is no longer necessary for the purpose which you originally collected or processed it for;
* The consent given which provides our lawful basis for holding the data, is withdrawn; (should be noted that in certain cases this information maybe considered a vital interest for the individual and therefore provide a basis for data to be retained)
* We are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
* We are processing the personal data for direct marketing purposes and the individual objects to that processing;
* We have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);
* We have to do it to comply with a legal obligation; or
* We have processed the personal data to offer information society services to a child.

**The right to erasure does not apply if processing is necessary for one of the following reasons:**

* To exercise the right of freedom of expression and information;
* To comply with a legal obligation;
* For the performance of a task carried out in the public interest or in the exercise of official authority;
* For archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
* For the establishment, exercise or defence of legal claims.

**Do we have to tell other organisations about the erasure of personal data?**

CANTO will endeavour to contact each recipient of the data and inform them of the erasure, unless this proves impossible or involves disproportionate effort.

The GDPR defines a recipient as a natural or legal person, public authority, agency, or other body to which the personal data are disclosed.

**Right to portability**

GDPR gives the individual the right to ask for their data in a commonly used format, the individual may also request that this data is transmitted directly to another controller.  This right only applies to personal data and data that in the first instance has been provided to the college.  When the college receives a request for data to be passed on in this way it will ensure that it is: structured; commonly used; and machine-readable.

**Subject Access Requests**

A Subject Access Request is a request for personal information that is held by the college about an individual. If an individual wishes to exercise their subject access right, the request must be made in writing to the college. The purpose of a SAR is to make individuals aware of and allow them to verify the lawfulness of processing of their personal data. Under the GDPR and the current Data Protection Act (DPA), individuals have the right to obtain confirmation as to whether personal data is being processed. This request will be responded to within a period of 30 days.

An individual may request the following information from the college if personal information is being processed:

The description of the personal data concerning them

Anyone who has received or will receive their personal data

Details of the origin of their data if it was not collected from them.

The reasons why their data is being processed;

To ensure that CANTO Learning fully complies with GDPR no charge will be made for this service unless as per GDPR the request is *‘manifestly unfounded or excessive’*. Should this be the case the college may request a reasonable fee for this service.

The college also retains the right under GDPR to withhold personal data under GDPR should disclosing it *‘adversely affect the rights and freedoms of others.*

All Subject Access Request should be made in the first instance to a member of the SLT.

**CCTV**

To maintain the security of the college and site CANTO instructs a third party to maintain a CCTV system on its behalf.  The system is designed so that it will not provide facial recognition but is used to identify and deter criminal activity.  Our third party maintain this system in line with their Data Protection/GDPR policy and procedures.  As per their policy images captured will be stored for 30 days unless specified by CANTO Learning and in the case of criminal activity will be stored for 60 days.  Should a need a rise to share images with authorities these will be done securely.  As per our operators policy all images and alerts are destroyed/deleted after a period of 60 days.

**Attendance System**

Our attendance monitoring systems fully complies with DPA 2018 and the GDPR through security measures installed and design of operating system. By following guidance from the third party supplier we are confident that we fully comply with all requirements. To further support this we request that all students either opt in or out on an annual basis re the use of this system.  Regular checks are undertaken to ensure that the system is maintained in line with current permissions.

**Breach Notification**

CANTO Learning Ltd recognises that in the event of a data breach certain actions must take place.  Should a data breach occur as in the case of a loss, theft, unauthorised access etc actions followed must meet GDPR standards. Critical to this is the reporting of the breach to supervisory authority (ICO) within 72 hours. If it is assessed that the breach is such that it places the data subject at a high privacy risk the individual should be informed of the breach within the same period.

**Records Management \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Introduction**

CANTO Learning Ltd is committed to managing its records, in whatever format, to minimum agreed standards.  This Policy establishes how the college will manage its records.  It also defines the roles and responsibilities for the creation, storage, access, amendment and disposal of college information.  This document provides the policy framework through which this effective management can be achieved and audited.

**It includes:**

* [Aims](https://www.keele.ac.uk/recordsmanagement/recordsmanagementpolicy/#Aims)
* [Scope](https://www.keele.ac.uk/recordsmanagement/recordsmanagementpolicy/#Scope)
* [Definitions](https://www.keele.ac.uk/recordsmanagement/recordsmanagementpolicy/#Definitions)
* [Responsibilities](https://www.keele.ac.uk/recordsmanagement/recordsmanagementpolicy/#Responsibilities)
* [Relationship with existing policies](https://www.keele.ac.uk/recordsmanagement/recordsmanagementpolicy/#Relationship)
* [Storage](https://www.keele.ac.uk/recordsmanagement/recordsmanagementpolicy/#Storage)
* [Disposal](https://www.keele.ac.uk/recordsmanagement/recordsmanagementpolicy/#Disposal)
* [Available Guidance](https://www.keele.ac.uk/recordsmanagement/recordsmanagementpolicy/#Available)

**Aims**

The aim of this policy is to consolidate a consistent approach to Records Management across all functions within the college and establish requirements designed to help staff meet legal obligations relating to Records Management.

It will ensure that non-essential records are destroyed in a consistent and confidential manner in line with the college’s disposal schedule.  It allows the college to identify what it retains as a permanent record of its activities.  The schedule also enables the destruction of those records which have outlived their administrative usefulness and are without significance for the historical or legal record.

**Scope**

This policy applies to all records created, received or maintained by staff of the college in the course of carrying out their function.  These records may exist in printed or digital form.

**Definitions**

**Records** are defined as: ‘Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.  This is any information, regardless of format or medium, captured in a reproducible format.

A **document** is any piece of written information in any form, produced or received by an organisation or person.

**Note** all records start off as documents, but not all documents will ultimately become records.

**Records Management** is the creation, maintenance, control, storage and disposal of records in a way which facilitates their most appropriate, efficient and effective use.

A **Disposal Schedule** is a list of records and the appropriate time limits that they must be kept for before they can be confidentially destroyed or transferred to archives for permanent storage. This document also defines which area of the college is responsible for the storage and disposal of records.

**Responsibilities**

The college has a responsibility to maintain its records and record-keeping systems in accordance with the regulatory requirements. **The Head of Centre and GDPR Lead** have responsibility for the implementation of the Records Management procedure within CANTO Learning Ltd.

The SLT is responsible for ensuring good practice in Records Management and promoting compliance with this policy.

Our IT 3rd party are responsible for ensuring that appropriate systems are provided to ensure the security of data held electronically, and that is backed up in accordance with agreed

contracts.

All College staff who create, receive and use college records hold Records Management responsibilities.  All members of staff are responsible for ensuring they exercise good Records Management in their daily working practice, which includes:

* The creation and maintenance of accurate and reliable records, where applicable to their role
* Ensuring electronic records are properly maintained and that they capture core information and remain accessible, readable and authentic
* Ensuring the security of records, irrespective of format, and for ensuring that access to records is only granted to those who are permitted to view them
* Following guidance provided in the Records Disposal Schedule with regard to the retention and disposal of records
* Ensuring records of a sensitive or personal nature are handled appropriately and in accordance with legal requirements

**Storage**

Records should be appropriately stored with due regard for efficiency, cost-effectiveness, security, durability and access. Appropriate procedures and processes should be put in place to ensure the physical and intellectual security of college records.

Storage conditions and handling processes should be designed to protect records from unauthorised access, loss or destruction and from theft and disaster.

**Disposal**

Records should be disposed of in accordance with agreed retention schedules.  The retention schedule should be reviewed regularly and adjusted if necessary.



Records and Data Retention Schedule

The college records and data retention schedule is a list of specific categories of records and how long they should be retained.  The Schedule covers records used for business and administrative purposes and helps promote consistent practice by ensuring records are kept for the same amount of time.

The college will retain personal data securely and only in line with how long it is necessary to keep for a legitimate and lawful reason. Typically, the legal recommendation for how long to keep ordinary staff and pupil personnel files is up to 7 years for staff and 10 years for students following departure from the college. However, incident reports and safeguarding files will need to be kept much longer, in accordance with specific legal requirements. If you have any specific queries about how this policy is applied, or wish to request that personal data that you no longer believe to be relevant is considered for erasure, please contact our GDPR Lead (Haydn Dear). However, please bear in mind that the college may have lawful and necessary reasons to hold on to some data.

**Why is using the Schedule important?**

CANTO Learning Ltd has legal and regulatory obligations to dispose of certain records after a set period of time. Effective records and data retention policies help underscore compliance with the General Data Protection Regulation (GDPR) and the Freedom of Information Act 2000.

**Access to retention schedules**

The Records and Data Retention Schedule covers both paper and electronic records - the format is irrelevant when deciding whether or not a record should be retained.

**Table of Retention Periods**

|  |  |
| --- | --- |
| **Type of Record/Document**   | **Retention Period**  |
| **COLLEGE-SPECIFIC RECORDS**  **Registration documents of College**   **Attendance Register**   **Minutes of Trustees' meetings** **Minutes of Senior Leadership Meetings****Minutes of Leadership Meetings****Minutes of Team/Group Meetings**  **Annual curriculum material, schemes of work etc.**  **Timetables and other session records, work.**  **Car Mileage logs**   |   **Permanent (or until closure of the college)**  **10 years from last date of entry, then archive.**  **For the length of the organization, in some form.** **10 Years/ For the length of the organisation in some form****3 Years****3 Years****From end of year: 3 years**   **From end of year: 1 year**    **6 years**  |
| **INDIVIDUAL STUDENT RECORDS**    **Initial Interview form and other supporting documents, pre-programme assessments etc.**  **Initial Interview and other documentation for non-starters.**   **Assessment results (record from awarding body)**  **Pupil file including:** **• Student ILP & reviews** **• Student Daily Record Sheets** **• Medical information** **• Assessment material: STAR assessments, work experience assessments**  **Any EFS funded programmes (Brighter Furtures, E2E)**    |     **10 Years as part of programme file.**    **Current year + 1 academic year.**    **10 years**   **10 Years**  **Should any material be relevant to another matter/claim this should be held for a longer period (advice to be sought at the time).**  **25 years**  |
| **SAFEGUARDING**   **Policies and procedures**     **DBS disclosure certificates staff/volunteers (if held)**       **Accident / Incident reporting**         **Child Protection files**   |    **Keep a permanent record of historic policies**    **No longer than 6 months from decision on recruitment.** **A record of the checks made must be kept (to go on staff file when archived)**    **Keep on record for as long as any  victim may bring a claim (Advise should be sought to assess appropriate period.). Files should be reviewed if resources allow and a suitably qualified person is available.**   **If a referral has been made & social care have been involved or if the student has been subject of a multiagency plan – Indefinitely.**  **If low level concern, with no multi-agency action – apply applicable school low-level concerns policy rationale (this may be 7 years from end of programme OR indefinitely).**   |
| **ACCOUNTING RECORDS**  **Accounting records**    **Tax returns** **VAT returns** **Budget and internal financial reports**  |   **Minimum – 7 years from the end of the financial year in which the transaction took place**  **Minimum – 7 years** **Minimum – 7 years** **Minimum – 3 years**  |
| **IP / IT agreements (including software licences and ancillary agreements eg maintenance; storage; development; coexistence agreements;**  | **Minimum – 7 years from completion of contractual obligation concerned or term of**  |
| **EMPLOYEE / PERSONNEL RECORDS**   **Single Central Record of employees**    **Contracts of employment**   **Employee appraisals or reviews**   **Staff personnel file**   **Payroll, salary, maternity pay records** **Pension or other benefit schedule records**  **Job application and interview/rejection records (unsuccessful applicants)**  **Immigration records**  **Health records relating to employees**   |    **A permanent record is kept to show that all mandatory checks have been undertaken.**  **7 years from effective date of end of contract**  **Duration of employment plus 7 years**  **7 years unless documentation need in regard to other matter/claim**  **Possibly permanent, depending on nature of scheme**    **Minimum 3 months but no more than 1 year**   **Minimum – 4 years**  **7 years from end of contract of employment**  |
| **INSURANCE RECORDS**  **Insurance policies (will vary – private, public, professional indemnity)**     **Correspondence related to claims/renewals/ notification re: insurance**   |   **Duration of policy (or as required) To be kept on record until possible that no living person could make a claim.**    **Minimum –  7 years**  |
| **ENVIRONMENTAL & HEALTH RECORDS**  **Maintenance logs**  **Accidents to students**   **Accident at work records (staff)**    **Staff use of hazardous substances**   **Risk assessments (carried out in respect of above)**     |    **10 years from date of last entry**  **Until the age of 25, or for 10 years (unless safeguarding incident)**  **Minimum – 4 years from date of accident, but review case-by-case where possible**  **Minimum – 7 years from end of date of use**  **10 years.**  |

**Updates:**

**­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Data Protection and GDPR Policy:**

Updated 19th June 2019 - HD

Updated April 2020 - HD

Updated April 2021 - HD

Updated January 2022 – HD

Updated October 2022 - HD

**Records Management Policy:**

Updated 29th May 2019 – HD

Updated May 2020 – HD

Updated October 2022 - HD

**In September 2021, the Data Protection Policy/GDPR, Records Management Policy, were updated and combined making one Policy by HD.**