Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Data Protection Handbook

tcd.ie/dataprotection

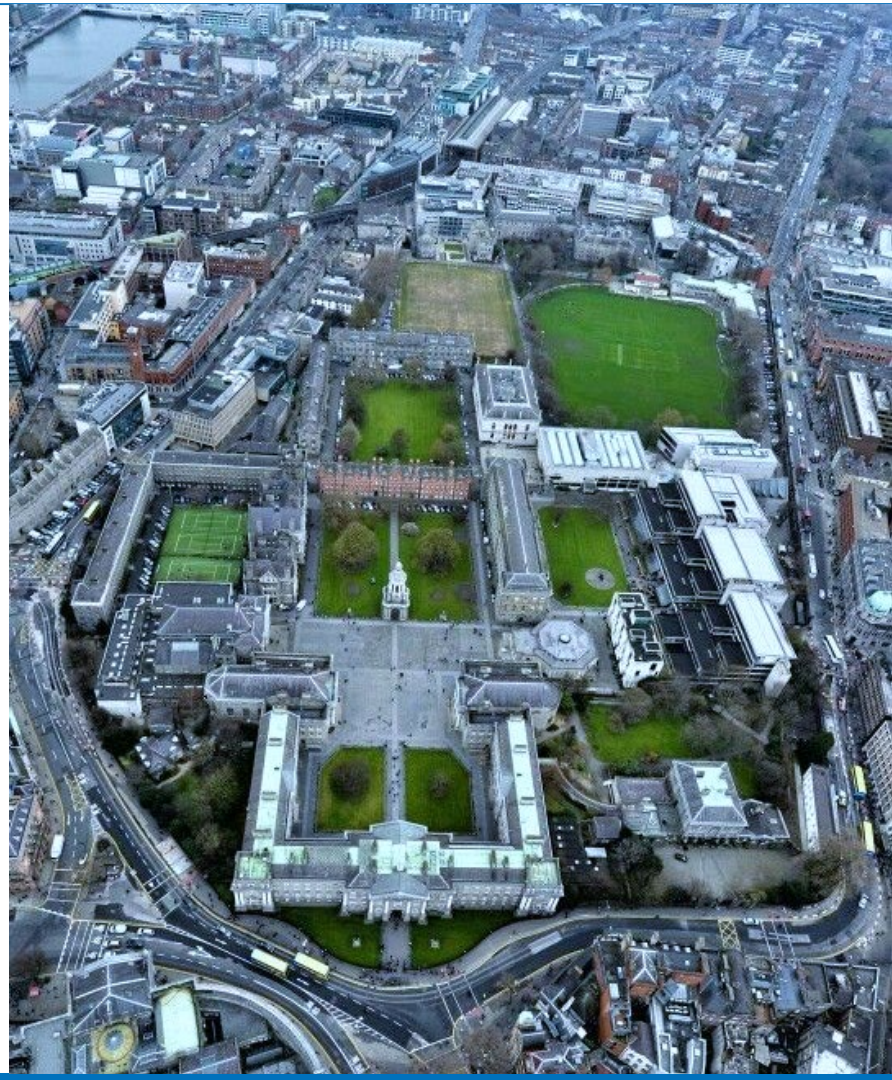
Contents

Introduction

Trinity College Dublin, the University of Dublin ('Trinity College'/'the University') acquires, processes, uses, discloses (where permissible by law) and retains personal data of individuals when carrying out its functions.

These individuals include students, staff, research participants, members of the public and other persons who engage with the University.

This protection of personal data is a fundamental right and is regulated by Irish and European data protection legislation, specifically the Data Protection Act 2018 and General Data Protection Regulation (GDPR) (EU) 2016/679 which strengthen the rights of individuals and place specific data processing obligations on organisations.



Glossary

PERSONAL DATA

Any information relating to an identified or identifiable person ('data subject').

PROCESSING

Any operation which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, storage, use, sharing, erasure or destruction.

Examples include:

- Email communication
- Videoconferencing calls
- Online teaching, learning and assessment, including streaming and recording of classes
- Managing files containing personal data, either in paper or electronic format

DATA SUBJECT

An individual 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 individual.

DATA CONTROLLER

An entity which determines the purposes and means of the processing of personal data. Trinity College is a data controller in relation to personal data relating to its staff and students.

DATA PROCESSOR

An entity which processes personal data on behalf of the controller. In certain instances Trinity College is a data processor when providing a service to another entity (e.g. analysis of data on behalf of a third party).

Glossary

SPECIAL CATEGORIES OF PERSONAL DATA

Data revealing a data subject's racial or ethnic origin, political opinions, religious beliefs or philosophical beliefs, data relating to trade union membership, genetic data, biometric data for the purpose of uniquely identifying a data subject, data concerning health and data concerning a data subject's sex life or sexual orientation. Further information available here.

PERSONAL DATA BREACH

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.

PSEUDONYMISATION

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 person.

ANONYMISATION

Irreversibly and effectively anonymised data is not 'personal data' and is not subject to data protection legislation. However, if the source data is not deleted at the same time that the 'anonymised' data is prepared, where the source data could be used to identify an individual from the 'anonymised' data, the data may be considered only 'pseudonymised' and thus still 'personal data' and subject to data protection legislation.

Examples of Personal Data

If someone can be identified directly or indirectly from information then it should be considered as personal data, and subject to data protection law

- Names of data subjects
- Contact details (e.g. Home address, Phone number, Email address)
- Online identifiers (e.g. IP address)
- Photographs, Video images, Voice recordings
- Date of birth/Age
- Birthplace, Citizenship, Ethnicity, Nationality, Gender
- Student/staff numbers
- CVs
- Details of gifts/donations made
- References for staff/students
- Location data
- Swipe card data (access controls)
- Trade Union membership
- Examination/assignment results
- Qualifications, Membership of professional associations
- Signatures (including e-signatures)
- PPS numbers
- Personal financial data (e.g. Bank account details, Income, Salary)
- Passwords, Pass codes, PIN numbers
- Data concerning health
- Research participant consent forms
- Clinical files relating to research participants
- Fingerprints, Biometric data
- Employment history including performance history/grievance/disciplinary details
- Next of kin details
- Data relating to children

Key Considerations

Please consider the following points before embarking on any activity involving the processing of personal data or the sharing of personal data with a third party

1. Do you really need to process personal data to meet your objective? Are there alternative ways that the same objective could be achieved without processing personal data?
2. Could anonymised or pseudonymised data be processed instead of data which directly identifies individuals? It is important to note that fully anonymous data is not considered as personal data and is not subject to data protection legislation.
3. Are you familiar with the key, core principles of data protection?
4. Do you have a valid justification for processing the data?
5. Has the data subject been informed of the processing i.e. issued with a privacy notice?
6. Have you taken all necessary measures to ensure that that the personal data will be secure during the process?

Key Considerations

Please consider the following points before embarking on any activity involving the processing of personal data or the sharing of personal data with a third party

7. Are you using software, systems and processes under the control of Trinity College?
8. Have you identified a legal basis for processing?
9. Have you completed training in data protection and IT security?
10. Do you know exactly what amount of data will be required to fulfil your objectives?
11. Have you determined an appropriate retention period for the data?
12. If sharing with third parties are the necessary contracts in place?
13. Are you planning to transfer the data outside the EEA? If so, do you have the necessary safeguards/permissions in place to do this?
14. If you are setting up new systems or processes have you conducted a Data Protection Risk Assessment or Data Protection Impact Assessment to measure risk associated with processing?

If processing of personal data is necessary, then the information in the following sections will provide more detail about the actions and considerations to be taken to ensure the processing meets the requirements of data protection legislation.

For further assistance and support please visit the Trinity College Data Protection website.

Principles of Data Protection

Please ensure to process personal data at all times in accordance with the core principles of data protection

1. LAWFULNESS, FAIRNESS AND TRANSPARENCY

Any processing of personal data should be lawful and fair. It should be transparent to data subjects as to how and to what extent their personal data is collected and processed. The principle of transparency requires that any information and communication relating to the processing of personal data is accessible and easy to understand, and that clear and plain language is used.

When Trinity College collects personal data directly or indirectly from data subjects, it must provide information regarding the intended processing to the relevant data subject. This information must be provided via a Privacy Notice. In addition, the University must have a legal basis as set out under Article 6 GDPR for processing personal data.

2. PURPOSE LIMITATION

Personal data should be processed by Trinity College for specified, explicit and legitimate purposes and not further processed by the University in a manner that is incompatible with those purposes.

3. DATA MINIMISATION

Processing of personal data should be adequate, relevant, and limited to what is necessary. Trinity College staff should periodically review processing activities to check that the personal data that is retained is relevant and adequate for the intended purposes and delete anything that is no longer required.

Principles of Data Protection

Please ensure to process personal data at all times in accordance with the core principles of data protection

4. ACCURACY

Trinity College must ensure that personal data is accurate and up to date; taking every reasonable step to ensure that inaccurate personal data is erased or rectified without delay.

5. STORAGE LIMITATION

Personal data should only be kept in a form which permits identification of data subjects for as long as is necessary for the purposes for which the personal data are processed. Trinity College has implemented a Records Management Policy and Records Retention Schedule which set out the University's policy on the creation and management of records, including records containing personal data.

Further information is available here.

6. INTEGRITY AND CONFIDENTIALITY

Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including protection against unauthorised or unlawful access, use or disclosure. Furthermore, Trinity College-controlled equipment which is used for the processing of personal data must be protected against accidental loss, destruction or damage, using appropriate technical or organisational measures.

ACCOUNTABILITY

Trinity College is responsible for, and must be able to demonstrate, compliance with each of the principles of data protection when processing personal data. Accountability responsibilities should be regarded as perpetual and will assist in mitigating data breaches and ensuring continual compliance with data protection law.

Legal Basis for Processing Personal Data

You must process personal data under an appropriate legal (lawful) basis, where at least one of the following conditions is met:

- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the University;
- the individual has consented to processing;
- processing is required due to a contract;
- processing is necessary for compliance with a legal obligation;
- processing is necessary to protect an individual's vital interests; or
- processing is necessary for the legitimate interests of the University or a third party and does not interfere with the rights and freedoms of individuals.

Trinity College is classified as a public body under the Universities Act, 1997. As such, the use of the 'legitimate interests' condition is not applicable to Trinity College's statutory functions but may be relied-upon as a legal basis for processing that is not related to the University's statutory functions.

Legal Basis for Processing Personal Data - Consent

Where Trinity College relies on consent as a legal basis for processing personal data, the University must:

- obtain the individual's specific, informed and freely given consent;
- ensure that the individual gives consent by a statement or clear affirmative action;
- retain evidence of that statement/affirmative action; and
- allow the individual to easily withdraw their consent at any time if they so wish.

It is recommended that consent is obtained in writing or electronic format. However, where consent is obtained verbally it is recommended that you use scripts and checklists to ensure that all necessary requirements have been met and that consent is obtained compliantly and can be evidenced.

The processing of special categories of personal data (sensitive personal data) requires additional conditions to be met pursuant to Article 9 GDPR and sections 45-55 of the Irish Data Protection Acts 1988-2018. Please see here for detailed information.

Data Security

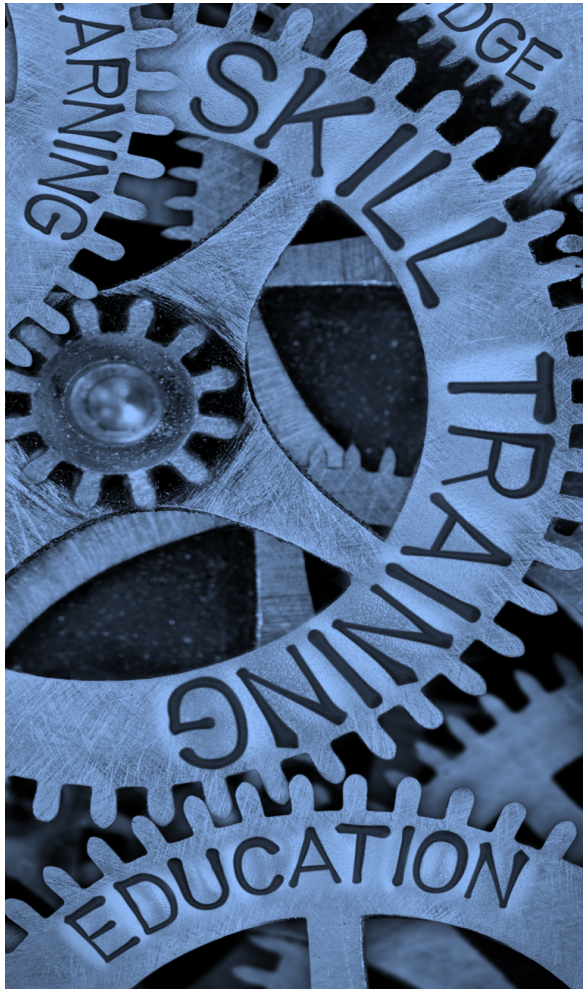
Trinity College implements appropriate technical and organisational measures to preserve data security and mitigate risk in order to safeguard University Information Systems and ensure the security, confidentiality and integrity of data under the control of Trinity College.

Personal data under the control of Trinity College should be processed in accordance with the University's IT Security Policy and Records Management Policy.

University-controlled data processed using Cloud-based services must be managed in accordance with the University Cloud Computing Policy and Guidelines.

Comprehensive information on Trinity College IT security provisions, including IT security policies, e-mail security guidance, cloud computing, training, data backup and encryption is available from the Trinity College IT Security website:

https://www.tcd.ie/ITSecurity

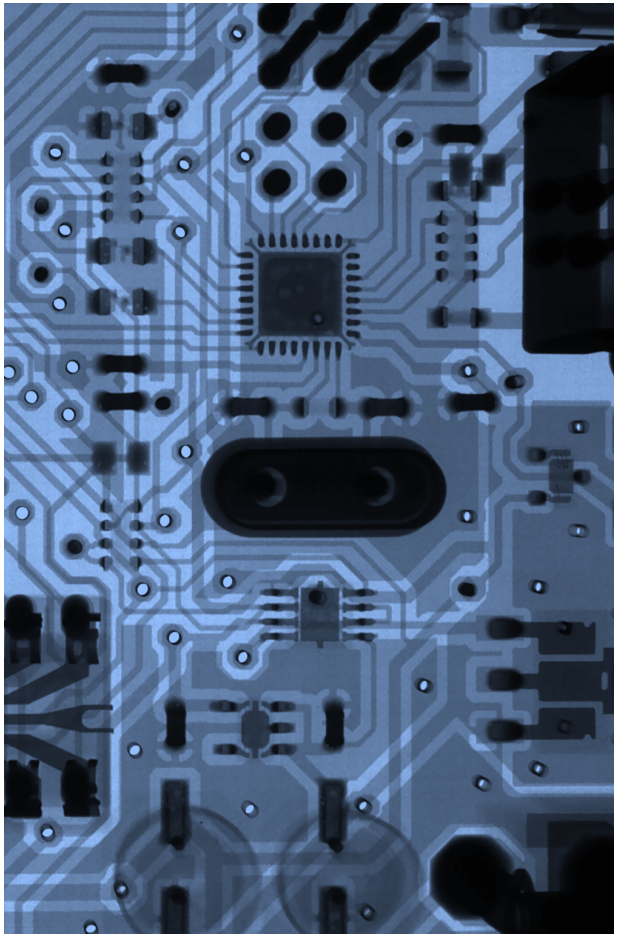


Data Security

Article 32 GDPR requires that an appropriate level of security must be implemented to prevent personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access.

The following technical and organisational measures should be implemented as appropriate:

- The pseudonymisation and encryption of personal data.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- The implementation of processes to regularly test, assess and evaluate the effectiveness of technical and organisational measures for ensuring the security of the processing.



Data Security – Good Practices

Technical measures alone are not sufficient to protect and secure personal data. Even if using secure software systems and devices, use safeguards and good practices when processing personal data.

- It is important to use Trinity-controlled and approved devices, IT systems and software when processing personal data on behalf of the University. Failure to do so results in the data being managed outside of the control of the University and may lead to data being lost, mislaid, stolen or disclosed as a consequence of accidental or malicious action. Do not use personal accounts for work purposes.
- Processing of confidential or sensitive personal data, such as HR-related data, student LENS Reports or data concerning health should be carried out only in circumstances where the data can be adequately safeguarded.
- Effective security measures not only involve protecting data from accidental or unlawful destruction, loss, alteration, or unauthorised disclosure, but also ensure that data can be retrieved and restored following an incident.
- Use strong passwords to combat hacking and change your passwords regularly. When updating your login password avoid using easy-to-guess passwords or passwords that are similar to previous versions.
- If using your phone / tablet for work purposes (e.g. using Office 365) make sure that the passcode is activated.

Data Security – Good Practices

Technical measures alone are not sufficient to protect and secure personal data. Even if using secure software systems and devices, use safeguards and good practices when processing personal data.

- Avoid sharing files to your computer's hard drive – save to the Cloud or to the Shared Drive instead.
- Use trusted computers and Wi-Fi connections and use VPN where appropriate.
- Avoid making copies where possible and delete / shred duplicate data (electronic & paper-based) - Use a confidential bin or shredder when disposing of documents containing personal data.
- Ensure that your laptop or desktop is encrypted (contact IT Services for more information on how to get your computer encrypted free of charge).
- Back up your data regularly and keep your anti-virus software up to date.
- Lock your computer when leaving your desk by pressing 'Ctrl, Alt, Delete'.
- Keep documents and devices which contain personal data secure when working at home.
- Do not visit untrusted websites, do not sign-up for notifications or open emails from untrusted organisations.

Best Practice When Using Email

Owing to the high volume of email usage as part of day-to-day operations it is necessary to follow the advice below when using Microsoft Outlook for College purposes.

- Ensure that you are emailing the correct address. When sending emails remember to double-check the address of the recipient(s) and pause to be sure before pressing 'send'.
- Avoid using email for filesharing activity. Use Microsoft OneDrive or SharePoint instead. This is especially important if you are sending sensitive or confidential data.
    - Further information on how to use OneDrive is available here.
    - Further information on how to use SharePoint is available here.
- When emailing large numbers of recipients always use the 'BCC' field to prevent recipients from identifying one another.
- If sharing attachments via email, encrypt or password protect the documents before emailing.
- When updating your login password avoid using easy-to-guess passwords or passwords that are similar to previous versions.
- Clear out your mailbox to reduce clutter. Organise emails into secure folders and delete excessive and duplicate data.

Best Practice When Using Email

Owing to the high volume of email usage as part of day-to-day operations it is necessary to follow the advice below when using Microsoft Outlook for College purposes.

- Use a Confidentiality Note with your email signature. Contact dataprotection@tcd.ie for a template version.
- Stay vigilant. Keep an eye on your email account and be aware of potential phishing scams.
- Never open an email attachment or click on a link from an untrusted source. If you see something unfamiliar it could be a sign that your account has been compromised - contact itservicedesk@tcd.ie immediately in such instances.
- Do not use personal email accounts for College purposes.
- Avoid writing personally-held views or opinions in emails.
- If using your phone / tablet for sending and receiving emails make sure that the passcode is activated.
- Contact dataprotection@tcd.ie immediately in the event of an incident involving personal data loss or disclosure.

Reporting a Data Breach

Under GDPR, a personal data breach is defined as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'. This definition extends to breaches which result from malicious conduct, lack of appropriate security controls, system or human failure, or error.

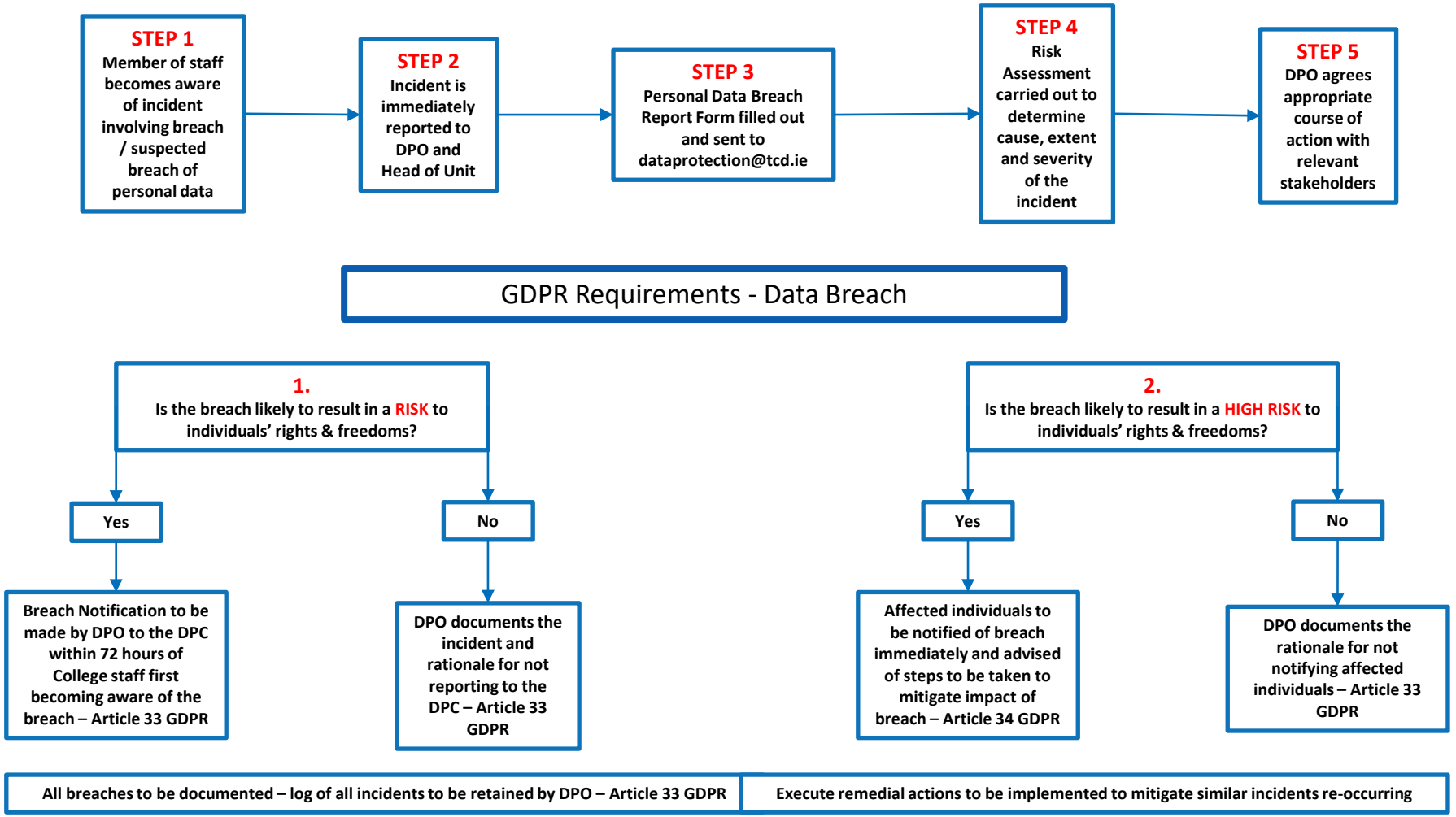
Where a data breach is likely to result in a risk to the rights and freedoms of data subjects, the College is required under GDPR to report the breach to the Data Protection Commission within 72 hours of discovery, even if the risk is not considered as substantial. Where appropriate, actions to inform individuals affected by the breach and reduce risks to their privacy arising from the breach will be implemented without delay.

These timeframes include weekend and public holidays and failure to comply will result in regulatory sanction and reputational damage for the College. As such, it is extremely important that you take immediate action upon learning of a breach or suspected incident involving the loss or disclosure of data and contact the Data Protection Officer and Head Of School or Unit without delay. All emails should be marked 'Urgent'.

Trinity College has implemented robust and documented controls for identifying, investigating, reviewing and reporting breaches or complaints. The University has developed Personal Data Breach Procedural Guidelines to assist staff in identifying and handling incidents involving personal data breaches. The Guidelines and Breach Report Form are available to download here.

Staff, students and associated entities who discover a personal data breach or suspected incident should inform the relevant Head of School / Unit and contact dataprotection@tcd.ie immediately.

Reporting a Data Breach - Procedure



Data Protection by Design and by Default

It is important that data protection is incorporated into systems and processes from the outset of processing as standard practice. This is achieved by embedding data privacy and security features, settings and controls directly into the design of University projects and systems.

- DATA PROTECTION BY DESIGN states that any action which an organisation undertakes that involves processing personal data must be done with data protection and privacy considerations in mind at every step. This includes internal projects, product development, software development and IT systems. In practice, this means that the University must ensure that privacy is built into a system during the whole life cycle of the system or process.

- DATA PROTECTION BY DEFAULT means that once a product or service has been released to the public, the strictest privacy settings should apply by default, without any manual input from the end user. In addition, any personal data provided by the user to enable a product's optimal use should only be kept for the amount of time necessary to provide the product or service.

Data Protection by Design and by Default

You can apply the principles of Data Protection by Design and by Default when processing any personal data by:

- Collecting, disclosing and retaining the minimum personal data for the minimum time necessary for the purpose;
- Anonymising or pseudonymising personal data wherever necessary and appropriate;
- Carrying out a Data Protection Risk Assessment ('DPRA') to determine risks associated with processing of personal data;
- Carrying out a Data Protection Impact Assessment ('DPIA') – see section below – where the processing is likely to result in a high risk to the rights and freedoms of individuals, especially when a new data processing technology is being introduced;
- Carrying out a DPIA where systematic and extensive evaluation of individuals is to be carried out based on automated processing (profiling), large scale processing of special categories of data and personal data relating to criminal convictions.

Data Protection by Design and by Default - DPIA

The DPIA is a mechanism for identifying and examining the impact of new initiatives or new technologies and putting in place measures to minimise or reduce risks. DPIA completion is required as a key component of system and process design, in particular where processing utilises new technologies and, taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of individuals.

A DPIA should include:

- A description of the envisaged processing operations and the purposes of the processing
- An assessment of the necessity and proportionality of the processing operations
- An assessment of the risks to the rights and freedoms of data subjects
- An outline of the measures to address the risks and demonstrate compliance

Examples of circumstances in which a DPIA is likely to be required include:

- Health Research as defined under the Health Research Regulations 2018
- Processing of large quantities of personal data
- Processing of special categories of personal data
- Where there is automatic processing/profiling of individuals

Data Protection by Design and by Default - Templates

Trinity College has developed the following template documents:

- DPRA Template - available here
- DPIA Templates for Research - available here
- DPIA Template for Non-Research (Services) - available here

Detailed information on DPIAs is available from the Data Protection Commission.

Staff and students intending to implement processes which may require a DPRA or DPIA should contact dataprotection@tcd.ie.

Staff and students intending to conduct research which may require a DPRA or DPIA should contact researchdpo@tcd.ie.

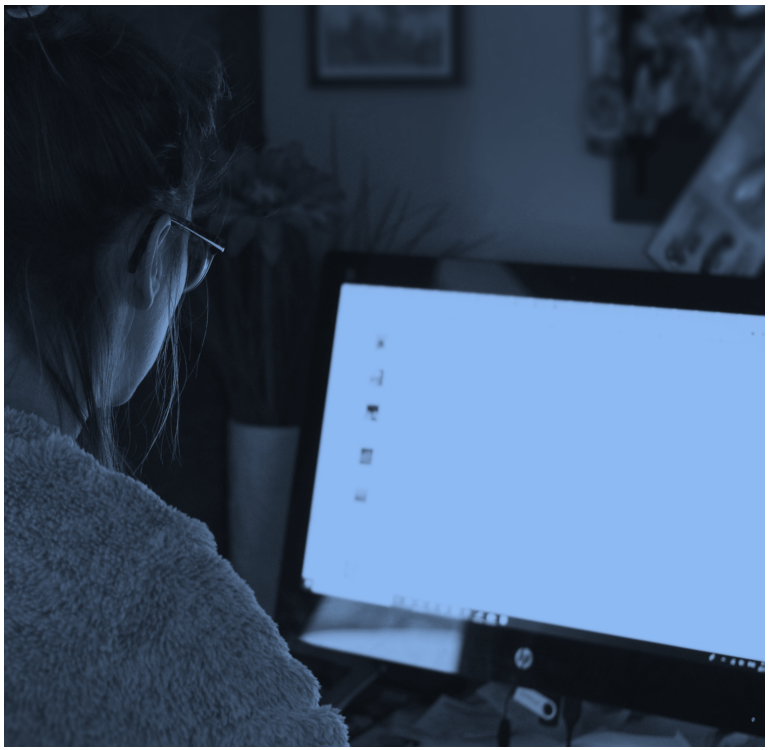
Data Sharing - Internal

Internal data sharing with colleagues within your own School, Unit or Institute or with colleague from another area within the University should only be carried out using University IT systems and in accordance with University policies.

Before sharing data, considered the following:

1. Is the sharing of personal data necessary?
2. Is the minimum amount of data being shared?
3. Is the data being shared with the appropriate recipient(s)?
4. Are you satisfied that the appropriate control mechanisms are in place for the data at its destination?

Avoid sharing large quantities of data (e.g. spreadsheets) or confidential / sensitive data via email. Use Microsoft OneDrive or SharePoint where appropriate.



Data Sharing - Third Parties

Trinity College shares data with partner organisations and engages the services of third party processors for certain processing activities.

The University carries out contractual due diligence when forming such business relationships and utilises information security audits to identify, categorise and record personal data that is processed outside of Trinity College's direct control, so that the data, processing activity, third party and legal basis are recorded, reviewed and easily accessible.

Such external processing and data sharing includes (but is not limited to):

- IT systems and services
- HR and Payroll services
- Partner institutes and organisations which take Trinity students on placement
- Access Control systems
- CCTV systems

Staff and students intending to transfer personal data to third party processors or sharing personal data with research partners should contact dataprotection@tcd.ie for support.

Data Sharing - International Data Transfers

The GDPR imposes restrictions on the transfer of personal data to third countries or international organisations located outside of the European Economic Area ('EEA'). These restrictions are in place to ensure that the level of protection and accountability afforded by GDPR is not undermined.

Personal data may only be transferred from Trinity College to entities situated outside of the EEA in compliance with the conditions for transfer as set out under Chapter V GDPR.

Staff and students intending to transfer personal data outside of the EEA, for example; using third party processors or sharing personal data with research partners should contact dataprotection@tcd.ie for support.

Data Retention

The GDPR requires Trinity College to retain personal data for as long as is necessary to serve the processing objectives. Generally, data should only be retained for as long as necessary and deleted when no longer required.

However, retention periods can differ based on the type of data processed, the nature and purpose of processing, and other factors.

It is important to ensure that agreed retention periods are approved and adhered-to. This means that data should be deleted, destroyed or fully anonymised at the end of the retention period or archived appropriately and securely.

Staff, students and researchers processing personal data should consult with the University Records Management Policy - available here - and Records Retention Schedule - available here - when determining appropriate retention periods for data.

Data Subject Rights

Data Protection and the preservation of individuals' rights under the legislation are considered as fundamental rights

THE RIGHT TO BE INFORMED

Data subjects have the right to be informed about the processing of their personal data. Where personal data is being collected directly from a data subject, a Privacy Notice must be provided at the point at which the data is collected.

The Privacy Notice should contain the following information:

- Who is collecting and processing the data (e.g. Trinity College School or Business Unit);
- Why the data is being processed;
- The legal basis (per Articles 6 and 9 GDPR) used to justify the processing;
- The format of the processing;
- How long the data will be retained;
- Who the data will be disclosed to; and
- How data subjects can exercise their rights under data protection law

Guidance on how to complete a GDPR-compliant Privacy Notice is available at:

https://www.tcd.ie/dataprotection/privacynotice/

Data Subject Rights

Data Protection and the preservation of individuals' rights under the legislation are considered as fundamental rights

THE RIGHT OF ACCESS

Data subjects are entitled to make an access request for a copy of their personal data. This data must be provided to the requestor free of charge within one month and in writing. Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the initial one-month period may be extended by two further months. However, this extension applies in exceptional circumstances only and the data subject must be notified of the reason for delay during the initial one-month period.

Data subjects wishing to make a request to access their personal data are advised to complete the Trinity College Data Access Form. Access requests received by University Schools and Business Units should be forwarded to the Data Protection Officer as soon as received.

The right to access one's own personal data is not absolute and is subject to restrictions. Where Trinity College does not comply with an access request the data subject must be informed during the initial one-month period of the reason(s) for the refusal and their right to lodge a complaint with the Data Protection Commission.

Guidance on how an access request should be fulfilled is available at:

https://www.tcd.ie/dataprotection/yourrights/

Data Subject Rights

Data Protection and the preservation of individuals' rights under the legislation are considered as fundamental rights

THE RIGHT TO RECTIFICATION

Personal data processed by Trinity College should be reviewed and verified as being accurate wherever possible. Where inconsistencies are identified by Trinity College, or where a data subject or other party informs the University of same, actions should be taken to ensure that such inaccuracies are corrected with immediate effect. All requests for rectification of personal data should be forwarded to the Data Protection Officer without delay.

THE RIGHT TO ERASURE (RIGHT TO BE FORGOTTEN)

The right to erasure, whereby data subjects can petition an organisation to have their data erased from its systems, is not absolute and only applies in certain circumstances.

Trinity College must respond to an erasure request as soon as possible. All requests for erasure of personal data should be forwarded to the Data Protection Officer without delay.

Data Subject Rights

Data Protection and the preservation of individuals' rights under the legislation are considered as fundamental rights

THE RIGHT TO RESTRICT PROCESSING

Trinity College may be required to restrict the processing of personal data under certain circumstances. Restricted data should be removed from the normal flow of information and recorded as such. The right to restrict processing is not absolute and only applies in certain circumstances. Trinity College must respond to a restriction of processing request as soon as possible. All requests for restriction of processing should be notified to the Data Protection Officer without delay.

THE RIGHT TO DATA PORTABILITY

This right allows data subjects to manage their personal data for their own purposes across different digital platforms and services. Data portability facilitates data subjects to transmit personal data between digital environments without hindrance to usability. All requests received regarding data portability should be forwarded to the Data Protection Officer.

Data Subject Rights

Data Protection and the preservation of individuals' rights under the legislation are considered as fundamental rights

THE RIGHT TO OBJECT

Data subjects have the right to object to:

- Processing of their personal data based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- Direct marketing (including profiling); and
- Processing for purposes of scientific/historical research and statistical purposes unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Data subjects should be informed of their right to object to processing in University Privacy Notices and at the point of first communication, in a clear and legible form and separate from other information.

In addition, Trinity College should provide opt-out options on all direct marketing material, whether conducted by Trinity College or by third parties on the University's behalf.

All requests regarding an objection to processing should be forwarded to the Data Protection Officer without delay.

Data Protection and Research

Trinity College promotes a Privacy by Design-based approach to any research project which uses personal or pseudonymised personal data. Adoption of this approach should minimise the risk of a data breach or non-compliance with data protection legislation.

Researchers at Trinity College should be aware of the provisions of, and operate in accordance with, data protection legislation. Researchers processing personal data for the purposes of health research should be especially mindful of the requirements of the Health Research Regulations 2018.

Any use of personal data or pseudonymised personal data for research must be in accordance with Article 9(2)(j) GDPR which states that processing should be 'necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.'

Data Protection and Research

Researchers must familiarise themselves with and adhere to University's Data Protection Policy, Good Research Practice Policy, procedures and guidance and should complete the relevant data protection training and research modules.

Researchers are encouraged to carry out DPIAs or DPRAs as appropriate and create data management plans for any research which uses personal data. This will ensure that the entire research journey from access/collection to deletion/archival has been considered from a data protection perspective.

The Deputy Data Protection Officer (Research) has developed a comprehensive suite of support documentation for researchers.

Please contact researchdpo@tcd.ie or visit https://www.tcd.ie/dataprotection/research for further information.

Training and Awareness

Trinity College has developed a suite of training and awareness material for the Trinity community:

- Online Data Protection Training for University staff. This training is a mandatory requirement for all staff who process personal data as part of their duties - available here.
- Online IT Security Awareness Training for staff - available here.
- Data Protection and Research - available here.
- Compulsory online module for Year 1 PhD students; CA7000: Research Integrity and Impact in an Open Scholarship Era, which includes sections on data protection, data management and research data security. For further information please contact niamh.brennan@tcd.ie.
- The University Data Protection Office has developed additional training materials in data protection for students and staff which are available on request. Please contact dataprotection@tcd.ie for further information.

Records of Processing Activities

Trinity College is required under Article 30 GDPR to maintain records of processing activities involving personal data and maintain such records (in writing) in a clear and easy to read format, to demonstrate the following:

- What personal data is processed
- Why it is processed
- Categories of the data subjects and the personal data
- How it was obtained
- The legal (lawful) basis for processing
- Where and how data is stored (including electronic and paper-based formats)
- Technical and organisational security measures in place to protect the data
- Who can access the data - recipients to whom the personal data have been or will be disclosed to
- Transfers of personal data to a third country or international organisation and documentation of the safeguards
- How long the data is retained for

Every School, Business & Support Unit and Research Unit at Trinity College is required to record its specific processing activities in accordance with Article 30 requirements. Further information on Article 30 requirements including relevant templates is available here.

Relevant Trinity College Resources

Data Protection Website - available here

Data Protection Policy - available here

IT Security Website - available here

IT Security Policy - available here

Privacy Notice - available here

Privacy Notice (Hybrid Learning) - available here

IT Services Crime Watch Hub - available here

IT Services Remote Learning Hub – available here

IT Services - Full List of Services - available here

Policy on Trinity Virtual Learning Environment - available here

Cookie Policy - available here

Web Policy Statement - available here

Dignity and Respect Policy - available here

Equality Policy - available here

Policy on Social Networking and Social Media - available here.

CCTV Code of Practice - available here

College Ethics Policy - available here

Article 9 GDPR Conditions for Processing of Special Categories of Personal Data

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited, unless one of the following conditions apply:

- The data subject has given explicit consent to the processing of their special category personal data for one or more specified purposes;
- The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- The processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subject(s);
- The processing relates to personal data which are manifestly made public by the data subject;

Article 9 GDPR Conditions for Processing of Special Categories of Personal Data

- The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- The processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- The processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to certain conditions and safeguards;
- The processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of data subjects, in particular professional secrecy;
- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) GDPR based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

tcd.ie/dataprotection