ITALIA CONTI

# Data Protection Policy

| | |
|---|---|
| Approved by: | Senior Leadership Team |
| Reviewed by: | Data Protection Officer and Quality Assurance Manager |
| Date of latest review | 18th June 2021 |
| Expiry date: | 19th June 2023 |
| | |

**This policy will be reviewed by SLT every 2 years unless there are legislative changes**

**Contents**

## 1. Aims

1.1. Italia Conti processes certain personal data about its employees, students and other stakeholders for a variety of specified and lawful purposes; these are identified in Privacy Notices issued to staff, students, alumni and others whose Personal Data it processes.[1] In order to protect the privacy of our stakeholders, and to comply with the principles laid out in law as set out below, Personal Data must be collected and used fairly, stored securely and confidentially, and destroyed when it is no longer needed.

1.2. Protecting the confidentiality, integrity and availability of personal data is a critical responsibility that we take seriously at all times. Confidentiality means that only people who have a need to know and are authorised to use Personal Data can access it. Integrity means that the Personal Data we process is suitable for the purpose for which it has been created/obtained. Availability means that authorised users are able to access Personal Data for authorised purposes.

1.3. Italia Conti aims to ensure that all Personal Data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and Processed lawfully in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

1.4. This policy applies to all Personal Data, regardless of whether it is in paper or electronic format.

## 2. Legislation

2.1. This policy reflects the requirements of the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018). It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.

2.2. It meets the requirements of the Protection of Freedoms Act 2012 when referring to Italia Conti's use of biometric data.

2.3. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

## 3. Definitions

3.1. **Staff**: all employees, workers, volunteers, governors and others acting on behalf of Italia Conti.

3.2. **Consent**: a freely given, specific, informed and unambiguous indication of a Data Subject's wishes by which the Data Subject, by a statement or clear affirmative action, signifies agreement to the processing of personal data relating to them, given by a clear positive action.

**3.3. Criminal Offence Data**: means Personal Data relating to criminal offences committed by an individual and offences alleged to have been committed, including proceedings for offences/alleged offences and the disposal of such proceedings, including sentencing.

3.4. **Data Breach (Personal)**: a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised access, disclosure or acquisition, of Personal

[1] https://www.italiaconti.com/policies/

Data.

3.5. **Data Controller**: the person/organisation that determines when, why and how to Process personal data. Italia Conti is the Data Controller of all Personal Data that we Process for our own purposes.

3.6. **Data Owners:** Directors responsible for key categories of Personal Data: Group Director of Institutional Effectiveness (student data), Group Director of HR (staff data), Group Director of Marketing (customers).

3.7. **Data Processor:** an external person or organisation who Processes Personal Data on our behalf.

3.8. **Data Subject**: a living, identified or identifiable individual about whom we Process Personal Data. Data Subjects may be nationals or residents of any country, who have legal rights regarding their Personal Data.

3.9. **Data Privacy Impact Assessment (DPIA)**: a tool to identify and reduce the risks of Personal Data Processing.

3.10. **Data Protection Officer (DPO)**: the person who has the responsibilities set out in GDPR Article 39 including monitoring Italia Conti's compliance with the GDPR/DPA 2018 and this policy, and providing advice and guidance relating to data protection.

3.11. **EEA**: the 27 countries in the EU, and Iceland, Liechtenstein and Norway.

3.12. **Explicit Consent**: Consent which requires a very clear and specific statement (that is oral or written and not just action).

3.13. **Personal Data**: any information relating to an identified or identifiable natural person (Data Subject); an identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, I.D. number, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental economic, cultural or social identity of that natural person e.g. email address, date of birth, an opinion about or intention regarding a person.

3.14. **Privacy Notices**: notices setting out information about the processing of personal data as prescribed by the GDPR Articles 13 and 14, which must be provided to Data Subjects when we collect their Personal Data.

3.15. **Processing or Process**: any activity that involves the use of Personal Data, including obtaining, recording storing, organising, amending, retrieving, using, disclosing, transferring, erasing, or destroying it.

3.16. **Pseudonymisation or Pseudonymised**: replacing identifying information with a pseudonym, so that the data subject cannot be identified without the use of information which is kept separately and securely.

3.17. **Related Policies**: Italia Conti's related policies, guidelines and procedures which are provided to assist in implementing this policy and are available on the Data Protection page of the Italia Conti website.

3.18. **Special Category Data**: Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health (physical or mental), sex life, sexual orientation, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, e.g., fingerprints, retina, and iris patterns.

## 4. The Data Controller

4.1. Italia Conti processes Personal Data relating to parents, pupils, staff, governors, visitors, and others, and therefore is a Data Controller.

4.2. Italia Conti is registered with the ICO and has paid its data protection fee to the ICO, as legally required.

## 5. Scope

This policy applies to all Staff who must ensure that their Processing of Personal Data on behalf of Italia Conti complies with its requirements regardless of the method of storage or type of Data Subject. This includes emails, notes and documents containing personal data. Breaches of this policy may result in disciplinary action or other appropriate action in respect of Staff who are not employees.

## 6. Roles and responsibilities

### 6.1. Governing board

The Board of Governors has overall responsibility for ensuring that Italia Conti complies with all relevant data protection obligations.

### 6.2. Data Protection Officer and Accountable Officer

The Data Protection Officer (DPO) for Italia Conti is currently Mr. Will Flanagan.

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on Italia Conti data protection issues.

The DPO is also the first point of contact for individuals whose data Italia Conti processes, and for the ICO.

Full details of the DPO responsibilities are set out in their job description.

Our DPO is contactable via following email address: DPO@italiaconti.co.uk

The Accountable Officer acts as a representative of the data controller on a day-to-day basis.

## 7. All staff

Staff are responsible for:

7.1. Collecting, storing and processing any Personal Data in accordance with this policy and data protection law;

7.2. Informing Italia Conti of any changes to their Personal Data, such as a change of address;

7.3. Contacting the DPO in the following circumstances:

- With any questions about the operation of this policy, data protection law, retaining Personal Data or keeping personal data secure;
- If they have any concerns that this policy is not being followed;

- If they are unsure whether or not they have a lawful basis to use Personal Data in a particular way;
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer Personal Data outside the European Economic Area (EEA);
- If there has been a Personal Data Breach;
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
- If they need help with any contracts or sharing personal data with third parties.

## 8. Core Principles

8.1. Italia Conti Staff should ensure that they comply with the following GDPR data protection principles.

8.2. These principles require that Personal Data are:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes (purpose limitation);
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is Processed (data minimisation);
- Accurate and, where necessary, kept up to date;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which it is processed (storage limitation);
- Processed in a way that ensures it is appropriately secure including protecting against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality);
- Not transferred to another country outside the EEA without appropriate safeguards being in place.

8.3. This policy sets out how Italia Conti aims to comply with these principles.

## 9. Collecting Personal Data

9.1. Italia Conti Processes (e.g. collects and uses) student Personal Data primarily for the purposes of providing education and training as set out in the Privacy Notice for students. Italia Conti also processes Personal Data relating to Staff who are employees for general employment-administration purposes and to comply with contracts of employment, and in respect of other categories of Data Subject, in accordance with the relevant Privacy Notices issued. Personal Data should be Processed only for the purposes identified in those Privacy Notices.

### 9.2. Lawfulness, fairness, and transparency

Italia Conti will only Process Personal Data where we have one of 6 ‘lawful bases’ (legal reasons) to do so under data protection law:

- The Personal Data needs to be Processed so that Italia Conti can **fulfil a contract** with the individual, or the individual has asked Italia Conti to take specific steps before entering into a contract;
- The Personal Data needs to be Processed so that Italia Conti can **comply with a legal obligation**;
- The Personal Data needs to be Processed to protect the **vital interests** of the individual or another person i.e. to protect someone's life;
- The Personal Data needs to be Processed for the performance of **a task in the public interest or exercise its official authority;**
- The Personal Data needs to be Processed for the **legitimate interests** of Italia Conti or a third party, provided the individual's rights and freedoms are not overridden;
- The individual (or their parent/carer when appropriate in the case of a pupil) has given **Consent.**

9.3. For Special Category Data, we will also meet one of the special category conditions for Processing under data protection law: [2]

- The individual (or their parent/carer when appropriate in the case of a student) has given **Explicit Consent;**
- The Special Category Data needs to be Processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law;**
- The Special Category Data needs to be Processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent;
- The Special Category Data has already been made **manifestly public** by the individual;
- The Special Category Data needs to be Processed for the establishment, exercise or defence of **legal claims;**
- The Special Category Data needs to be Processed for reasons of **substantial public interest** as defined by the DPA 2018 Schedule 1 Part 2 (e.g. safeguarding, preventing/detecting unlawful acts);
- The Special Category Data needs to be Processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person under a professional duty of confidentiality;
- The Special Category Data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person under a duty of professional duty of confidentiality;
- The Special Category Data needs to be Processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest;

9.4. For Criminal Offence Data, we must comply with one of the lawful bases as set out above in relation to non-Special Category Personal Data and also meet one of the conditions specific to Criminal Convictions Data as set out in the DPA Schedule 1. The DPA Schedule 1 conditions are similar to those that apply to Special Category Data including the substantial interest conditions provided by the DPA Schedule 1 Part 2. Some conditions, such as preventing or detecting unlawful acts or safeguarding of children explicitly require you to demonstrate that the processing is 'necessary for reasons of substantial public interest'. However, DPA Schedule 1 paragraph 36 removes this requirement for Criminal Offence Data, although the requirement remains in place for the processing of Special Category Data. So if Processing Criminal Offence

[2] Please refer to the Special Category and Criminal Offence Data Policy DRAFT 23.3.21.docx

Data only, and not Special Category Data, reliance can be placed on one of the listed conditions without needing to demonstrate that the Processing is necessary for reasons of substantial public interest.

**9.5. Conditions include:**

- The individual (or their parent/carer when appropriate in the case of a student) has given **consent.**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made **manifestly public** by the individual.
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise, or defence of **legal rights.**
- Whenever we first collect personal data directly from individuals, we will provide them with a Privacy Notice.
- We will always consider the fairness of our data processing. We will ensure we do not Process personal data in ways that individuals would not reasonably expect or use Personal Data in ways which have unjustified adverse effects on them.

**9.6. Limitation, minimisation and accuracy**

- Italia Conti will only collect Personal Data for specified, explicit and legitimate reasons, which must be set out in Privacy Notices when we first collect their data.
- If we want to use Personal Data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.
- Staff must only Process Personal Data where it is necessary in order to do their jobs and they should ensure that the Personal Data they college is relevant and proportionate.
- Staff should ensure that Personal Data is accurate and, where necessary, kept up-to-date. Staff should check the accuracy of Personal Data on collection and at regular intervals thereafter. Inaccurate Personal Data should be rectified or deleted without delay.
- In addition, when staff no longer need the Personal Data they hold, they must ensure it is deleted or anonymised.

## 10. Sharing Personal Data

10.1 Staff should not share Personal Data with anyone else unless there is a lawful basis for doing so. These include, but are not limited to, situations where:

- There is an issue with a student or parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:
- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.

- Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share.
- Only share data that the supplier or contractor needs to carry out their service. We ensure that the contract complies with the requirements for contracts with Data Processors as set out in GDPR Article 28 (3).

10.2 Italia Conti will also share Personal Data with law enforcement and government bodies where we are legally required to do so or where an exemption under the DPA 2018 applies.

10.3 Police requests for information:

Staff should always ask police authorities who make requests for personal data, (except in emergency situations), to do so via a "212" form signed by a senior officer.[3] This form should certify that the information is required for an investigation concerning national security, the prevention or detection of crime, or the apprehension or prosecution of offenders, and that the investigation would be prejudiced by a failure to disclose the information. This provides Italia Conti with a legal basis for supplying the data under the DPA exemptions.

10.4 Non-standard requests for legally required information from law enforcement agencies and government bodies:

- If a non-standard application is made, then Italia Conti will require the request to:
- Be in writing, on headed paper, and signed by an officer of the agency.
- Specify the type of information which is required - the categories and extent of the information requested should not be open-ended, and should be proportionate to the purpose.
- Describe the nature of the investigation (e.g., citing any relevant statutory authority to obtain the information).
- Certify that the information is necessary for the investigation.

10.5 Italia Conti may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff.

10.6 Where we transfer personal data internationally, we will do so in accordance with data protection law, in particular the provisions relating to transfers outside of the EEA as provided for in Articles 45-49. Transfers will only be made therefore if, for example:

- the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms;
- appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, (where applicable) a copy of which can be obtained from the DPO;

[3] A "212" form (issued under Schedule 2, Part 1, Paragraph 2 of the DPA) signed by a senior police officer will normally be required.

- the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
- the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

## 11. Subject access requests and other rights of individuals

11.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to their Personal Data that Italia Conti holds processes. This includes:

- Confirmation that their personal data is being processed.
- Access to a copy of the data.
- To be informed of the purposes of the Personal Data Processing.
- The categories of personal data concerned.
- Who the Personal Data has been, or will be, shared with (i.e. internal and external recipients or categories of recipient), in particular transfers outside of the EEA.
- How long the Personal Data will be stored for, or if this is not possible, the criteria used to determine this period.
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such Processing.
- The right to lodge a complaint with the ICO or another supervisory authority.
- Any available information on the source of the data, if not the individual.
- Whether any automated decision-making is being applied to their Personal Data, and what the significance and consequences of this might be for the individual.
- The safeguards provided if the Personal Data is being transferred internationally.

11.2 Subject access requests can be submitted in any form, but Italia Conti may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual.
- Correspondence address.
- Contact number and email address.
- Details of the information requested.

11.3 To make a 'subject access request', contact Italia Conti at **DPO@italiaconti.co.uk**.

If staff receive a subject access request in any form, they must immediately forward it to the Data Protection Officer (DPO).

## 12. Children and subject access requests

12.1 Children (i.e., those under 18) have reasonable expectations of privacy and therefore have the same rights as adults with regard to their Personal Data. For information relating to a student over and above that which a parent is entitled to receive under current legislation, a parent/ carer may make a subject access request on behalf of their child provided they have the child's consent or without the child's consent where the child is unable to understand their rights and the implications of a Subject Access Request.

12.2 Children below the age of 13 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students who are under 13 at Italia Conti may be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

12.3 Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students who are aged 13 and over at Italia Conti may not be granted without the express permission of the pupil. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

## 13. Responding to subject access requests

13.1. When responding to requests, we:

- May ask the individual to provide 2 forms of identification;
- May contact the individual via phone to confirm the request was made;
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant);
- Will provide the information free of charge;
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month and explain why the extension is necessary.

13.2. We may not disclose information for a variety of limited reasons, such as if it:

- might cause serious harm to the physical or mental health of the student or another individual;
- is requested by a person who is conferred with parental responsibility by a court because the child is unable to manage their own affairs, or it would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests;
- would include another person's Personal Data that we cannot reasonably anonymise, and we do not have the other person's consent and it would be unreasonable to proceed without it;
- is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

13.3. If the request is manifestly unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

13.4. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

13.5. Note: The DPO should be consulted before a subject access request is refused in reliance on any of the above grounds.

## 14. Other data protection rights of the individual

14.1. In addition to the right to make a subject access request (see above), and to receive information when we are collecting their Personal Data about how we use and Process it (see section 7), individuals also have the right to:

- Where processing is based on Data Subject's Consent, withdraw their Consent to Processing at any time. Consent should therefore only be relied on if there is no other lawful basis of Processing.
- Ask us to rectify, without undue delay, inaccurate Personal Data. In some circumstances, taking into account the purposes of the Processing of the Personal Data, an individual has the right to have incomplete Personal Data completed, including by means of a supplementary statement.
- In limited circumstances, have their Personal Data erased e.g., where Consent has been withdrawn and there is no other lawful basis for the Processing; the Personal Data is no longer necessary in relation to the purposes for which it was obtained; the individual objects to the Processing and there are no overriding legitimate grounds for the Processing or the individual objects to their Personal Data being Processed for direct marketing purposes;
- or restrict Processing of their Personal Data (this is a temporary measure in certain circumstances e.g., while a complaint regarding Processing is being considered).
- Prevent use of their Personal Data for direct marketing.
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests.
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their Personal Data with no human involvement).
- Be notified of a Personal Data Breach (in certain circumstances e.g. where the breach poses a serious risk).
- Make a complaint to the ICO.
- Ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

14.2. Individuals should submit any request to exercise these rights to the DPO using the email address: DPO@italiaconti.co.uk. If staff receive such a request, they must immediately forward it to the DPO.

## 15. Parental requests to see the educational record

15.1. Parents, or those with parental responsibility, have a legal right to free access to an annual written report of their child's progress and attainment in the main subject areas taught unless the parent has agreed otherwise.

## 16 Biometric recognition systems

16.1. Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

16.2. Where we use students' biometric data as part of an automated biometric recognition system, we will comply with the requirements of the Protection of Freedoms Act 2012.

16.3. Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. Italia Conti will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

16.4. Parents/carers and students have the right to choose not to use Italia Conti's biometric system(s). We will provide alternative means of accessing the relevant services for those students.

16.5. Parents/carers and students can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

16.6. As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the student's parent(s)/carer(s).

16.7. Where staff members or other adults use the Italia Conti's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and Italia Conti will delete any relevant data already captured.

## 17. CCTV

17.1. Italia Conti use CCTV in various locations around Italia Conti sites to ensure it remains safe. We will adhere to the ICO's Code of Practice for the use of CCTV.

17.2. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

17.3. Any enquiries about the CCTV system should be directed to the IT Manager, IT@italiaconti.co.uk.

## 18. Photographs and videos

18.1. As part of our Italia Conti activities, we may take photographs and record images of individuals within Italia Conti.

18.2. Consent is not required to use photographs/ videos for assessment purposes as such processing is necessary for the performance of the contract to provide the chosen academic programme.

18.3. Italia Conti will obtain written consent from both the parent and the student, where the student is under 18, or from students themselves if they are aged 18 and over, in respect of the use of photos/ videos for marketing purposes and will make students aware that their data is being used for this purpose.

18.4. Any photographs and videos taken by parents/carers at Italia Conti events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other students are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or students where appropriate) have agreed to this.

18.5. Where Italia Conti takes photographs and videos, uses may include:

- Within college on notice boards and in Italia Conti brochures, newsletters, etc.
- Outside of Italia Conti by external agencies such as the college photographer, newspapers, campaigns
- Online on the Italia Conti website or social media pages

18.6. Consent can be refused or withdrawn at any time. If consent is withdrawn, Italia Conti will delete the photograph or video and not distribute it further.

18.7. When using photographs and videos in this way we will not accompany them with any other personal information about the student, to minimise the likelihood that they will be identified.

18.8. Staff should also refer to the Italia Conti Safeguarding and Social Media policies for more information on our use of photographs and videos.

## 19. Data protection by design and default

19.1 Italia Conti will put technical and organisational measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only Processing Personal Data that is necessary for each specific purpose of Processing, and always in line with the data protection principles set out in relevant data protection law (see section 7).
- Completing Digital Processing Impact Assessment (DPIAs) where Italia Conti's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies. The general requirements relating to DPIAs are set out in Appendix 2 Staff should also contact the DPO to advise on specific assessments.
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Using Pseudonymised Personal Data rather names where practicable.
- Appropriate safeguards being put in place if we transfer any personal data outside of the European Economic Area (EEA), where different data protection laws will apply.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of Italia Conti and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices).
    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the EEA and the safeguards for those, retention periods and how we are keeping the data secure.

19.2 Individual members of staff should also ensure privacy by design and default in the way they manage Personal Data in discharging their day-to-day duties at Italia Conti, by taking appropriate steps to maintain security of personal data. Staff should therefore follow all procedures and use

the technologies Italia Conti has put in place to maintain the security of Personal Data from its creation/collection to its destruction. Staff must also maintain security of Personal Data by protecting the confidentiality, integrity and availability of Personal Data. Personal Data should be in Pseudonymised form.

19.3 Further information can be found in **Appendix 3: GDPR Guidelines for Italia Conti staff when working from home** and Appendix 4: **GDPR Guidelines for Italia Conti staff when working on-site.**

## 20. Storage Limitation

20.1. Italia Conti will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

20.2. Personal Data will not be kept for longer than is necessary for the purposes for which the data is processed, including for the purpose of satisfying any legal, accounting or reporting requirements.

20.3. Italia Conti will maintain a central Data Retention Procedure and Schedule, and each department or business area is required to maintain a local Retention Schedule which outlines the time for which personal data may be stored. Staff members must ensure that they delete personal data in line with both the central and local Retention Schedule, taking all reasonable steps to destroy or erase from all storage systems, including paper and electronic copies. This includes erasure of emails containing personal data and requiring third parties to delete such data where applicable.

## 21. Disposal of records

21.1. Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

21.2. For example, staff members will shred or incinerate paper-based records and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Italia Conti's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

## 22. Personal Data Breaches

22.1. Staff should make all reasonable endeavours to ensure that there are no Personal Data Breaches.

22.2. In the event of a suspected Personal Data Breach, the procedure set out in Appendix 1 must be followed.

22.3. When appropriate, Italia Conti will report the Personal Data Breach to the ICO within 72 hours after becoming aware of it. Such Personal Data breaches in an educational context may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person;

- The theft of a laptop containing non-encrypted Personal Data about students; or

22.4. Replying to all recipients of an email and including Special Category Personal Data which only one of the recipients needs to know, thereby inadvertently disclosing it to those who are not authorised to process it.

22.5. Further guidance on personal data breaches is provided in Appendix 1: Personal Data Breach Guidelines for staff ; Appendix 2: DPO Action Guidelines; Appendix 3: GDPR Guidelines for Italia Conti staff when working from home; Appendix 4: GDPR Guidelines for Italia Conti staff when working on-site.

22.6. Actions to minimise the impact of Personal Data Breaches

Italia Conti will take actions detailed in Appendix 2 to mitigate the impact of different types of data breach, focusing especially on Personal Data Breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any Personal Data Breach.

**22.7. Data breach helpline:**

Italia Conti also has insurance in place to mitigate any civil claims for data breaches. As part of this cover, a free helpline is provided by the underwriters. In the event of an actual or suspected cyber incident a call can be made to their Cyber Incident Response Team.

Please note: this helpline should only be used by the DPO where it is suspected that a breach might lead to a claim. Incidents such as sending emails to the wrong person do not need to be reported.

## 23. Training

23.1. All Staff and governors are provided with data protection training as part of their induction process.

23.2. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Italia Conti's processes make it necessary. Staff knowledge of the Data protection procedures will be refreshed annually.

## 24. Monitoring arrangements

24.1. The DPO and Quality Assurance Manager are responsible for monitoring and reviewing this policy.

24.2. This policy will be reviewed every **2 years** and shared with the Senior Leadership Team.

## 25. Links with other policies

25.1. This data protection policy is linked to our:

- Data Protection Impact Assessments (DPIAs) (Appendix 5 of this Data Protection Policy).
- Digital Safety Agreement (Juniors) https://italiacontiartscentreltd.sharepoint.com/:w:/s/ItaliaContiData/goswell-admin-share/EeR8hAaHhWdRi2lg2ja-x7MBQqYZLegFh1o0dU1L3lHwDg?e=qg5JK8
- Digital Safety Agreement (Seniors) https://italiacontiartscentreltd.sharepoint.com/:w:/s/ItaliaContiData/goswell-admin-share/EexPgIljpqhHrwCvTr4wf-QBjx02Op9E6nA3H1pJzRr5Og?e=ooWeyP
- Personal Data Breach Guidance for Staff (Appendix 1 of this Data Protection Policy)

- Processing of Special Categories of Personal Data and Criminal Offence Data Policy https://italiacontiartscentreltd.sharepoint.com/:w:/s/ItaliaContiData/goswell-admin-share/EckTBlcn6nZHt1f3ud-db-YBbwKyLidO-KsA8twvjAYtBw?e=fj9pbx
- GDPR Guidelines for Italia Conti staff when working from home (Appendix 3 of this Data Protection Policy)
- GDPR Guidelines for Italia Conti staff when working on-site (Appendix 4 of this Data Protection Policy)
- Privacy Notices (students, staff, alumni) including permission for biometric data collection and use. https://italiacontiartscentreltd.sharepoint.com/:f:/s/ItaliaContiData/goswell-admin-share/EnNAu2qpYTFKlkPspp-G7O0BhEHHeGigMurqkX-BUzK6Rw?e=NsQoWe
- E-Safety and internet policy https://italiacontiartscentreltd.sharepoint.com/:w:/s/ItaliaContiData/goswell-admin-share/EaervCmY6ehWlsXDlD6xojMB49zcKcFabb4sZUjtKdiv4g?e=bkwhiD
- Safeguarding Policy https://italiacontiartscentreltd.sharepoint.com/:w:/s/ItaliaContiData/goswell-admin-share/Ec_X8DcUrYZEjVRre2of0m8Bh2y2Gt45aZmQKlPx21OFmw?e=C5UdaJ
- SEND Policy https://italiacontiartscentreltd.sharepoint.com/:w:/s/ItaliaContiData/goswell-admin-share/ER7rusCBh65Spzw-cDRW0jEBw52bS57eSCgqX2q4iUzwKw?e=qsUmZD
- Social Media Policy https://italiacontiartscentreltd.sharepoint.com/:w:/s/ItaliaContiData/goswell-admin-share/EZCRb81SRtNdjfMv6BJ8OLIBay53JiJC6jotq8urGfQnNA?e=9Bqc4V

## Appendix 1: Personal Data Breach Guidelines for staff

These guidelines are to support staff where a suspected data breach has taken place.

You should approach data breach reporting in the same way that you approach safeguarding.

**Key terms:**

| | |
|---|---|
| Information Commissioner's Office | The organisation set up by the government to regulate data protection in England. |
| Data controller | The organisation (or individual) who is legally allowed to have access to personal information, in this case Italia Conti. |
| Personal Data | Any information relating to an identified or identifiable natural person (Data Subject); an identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, I.D. number, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental economic, cultural or social identity of that natural person e.g. email address, date of birth, an opinion about or intention regarding a person |
| Special Category Data | Personal Data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health (physical or mental), sex life, sexual orientation, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, e.g., fingerprints, retina and iris patterns. |
| Criminal Offence Data | Personal Data that relates to criminal offences committed by an individual and offences alleged to have been committed, including proceedings for offences/alleged offences and the disposal of such proceedings, including sentencing. |

What is a “personal data breach”?

The Information Commissioner’s Office (ICO) defines a “data breach” as being when “someone other than the Data Controller gets unauthorised access to personal data”. It can also involve someone getting unauthorised access within an organisation, or where an employee accidentally alters or deletes personal data. (Information Commissioners Office, 2020, pp. https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-breaches/#:~:text=A%20personal%20data%20breach%20may,alters%20or%20deletes%20personal%20data.)

A personal data breach occurs whenever any personal data is:

Lost
Destroyed
Corrupted
Disclosed
Made available to Individuals

Made unavailable – *and* this has a significantly negative effect on individuals.

} without proper authorisation

A personal data breach might be classed as “high risk” if it has “the potential of people suffering significant detrimental effect – for example, discrimination, damage to reputation, financial loss, or any other significant economic or social disadvantage” (Stinson, 2018, pp. https://www.tes.com/news/how-react-data-breach).

Examples include:

- Sending personal data to the wrong person.
- Losing a laptop with personal data on it.
- Leaving open a work email account that others can access.
- Losing a memory stick.
- Safeguarding information being made available to a non-authorised person.

## What to do if you suspect a data breach has taken place:

1) Notify the Data Protection Officer (DPO) at Italia Conti. Do this even if you are not sure whether the data disclosed was personal.
2) Send evidence of the disclosure, e.g. if the data breach involves an email, send the DPO a copy of that email.
3) Complete a *GDPR incident report form*. (The DPO will send you a copy).
4) The DPO will investigate and report on the incident.

Data Breach of sensitive information via email:

1) If sensitive information (including safeguarding records) is accidentally made available via email to unauthorised individuals, you must attempt to recall the email as soon as you become aware of the error.
2) Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.
3) If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it.
4) In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorized individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
5) The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.
6) The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

**Source documents:**

Information Commissioner's Office. (2020). security-breaches. Retrieved November 30th , 2020, from Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-breaches/#:~:text=A%20personal%20data%20breach%20may,alters%20or%20deletes%20personal%20data.

Stinson, J. (2018, May 12th). How-react-data-breach. Retrieved November 30th, 2020, from Times Educational Supplement: https://www.tes.com/news/how-react-data-breach

## Appendix 2: DPO action guidelines

The following measures apply to all potential personal data breaches:

The DPO will investigate the incident and will do the following:

1) Decide whether a personal data breach has occurred and assess the severity of the breach.
2) Alert immediately (where appropriate) the Senior Leadership Team (SLT). (If the breach is not deemed serious, the SLT will review the breach as part of the normal data breach reviewing process.
3) Where necessary (in the event of a sensitive personal data or a serious data breach), the ICO will be informed within 72 hours of the breach.
4) A record will be kept of the personal data breach (in case of any future challenge by the ICO or the individual(s) whose personal data has been breached). This will be recorded in the *GDPR Incident Log*.
5) Review the data breach incident as part of the normal review process with the SLT to determine what procedural modifications are needed to prevent a similar data breach in the future.

**If the severity is high**

6) The DPO will write to the individuals whose personal data has been breached.
7) The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
8) The DPO will document each breach, irrespective of whether it is reported to the ICO.
9) The DPO and Senior Management Team will meet as soon as possible to review what happened, and how it can be stopped from happening again.

**Data breach helpline:**

Italia Conti also has insurance in place to mitigate any civil claims for data breaches. As part of this cover, a free helpline is provided by the underwriters. In the event of an actual or suspected cyber incident a call can be made by the DPO to their Cyber Incident Response Team.

Source documents:

Information Commissioners Office. (2020). security-breaches. Retrieved November 30th , 2020, from Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-breaches/#:~:text=A%20personal%20data%20breach%20may,alters%20or%20deletes%20personal%20data.

Stinson, J. (2018, May 12th). How-react-data-breach. Retrieved November 30th, 2020, from Times Educational Supplement: https://www.tes.com/news/how-react-data-breach

## Appendix 3: GDPR Guidelines for Italia Conti staff (hybrid working)*

### Purpose:

To ensure that staff meet key privacy standards whilst using confidential information in the course of their duties.

### Aims:

Italia Conti processes certain personal data about its employees, students and other stakeholders for a variety of specified and lawful purposes; these are identified in Privacy Notices issued to staff, students, alumni and others whose Personal Data it processes.[4] In order to protect the privacy of our stakeholders, and to comply with the principles laid out in law as set out below, Personal Data must be collected and used fairly, stored securely and confidentially, and destroyed when it is no longer needed.

Protecting the confidentiality, integrity and availability of personal data is a critical responsibility that we take seriously at all times. Confidentiality means that only people who have a need to know and are authorised to use Personal Data can access it. Integrity means that the Personal Data we process is suitable for the purpose for which it has been created/obtained. Availability means that authorised users are able to access Personal Data for authorised purposes.

Italia Conti aims to ensure that all Personal Data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and Processed lawfully in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

This policy applies to all Personal Data, regardless of whether it is in paper or electronic format.

It should be read in conjunction with the Data Protection Policy and the Personal Data Breach Guidelines for Staff.

### Procedure:

- Microsoft Office™ is provided by Italia Conti via your email address. You should always log into Microsoft Office™ using your Conti email address, rather than your personal account.
- All emails connected to Italia Conti should be sent from your Italia Conti email address. You should not use your personal email account.
- You should minimise storing Italia Conti data on your personal device(s). This can be achieved by always using your Microsoft Office 365™ login to access and edit documents rather than downloading it to your local machine. Italia Conti provide access to a secure environment via Microsoft One Drive™ and Microsoft Share Point™. Information at setting Microsoft Share Point to automatically use your Microsoft applications on your machine can be found at: https://www.youtube.com/watch?v=hVpX4wQdIhc
- Keep any device you use password protected. Remember that strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers, and special characters (e.g., asterisk or currency symbol). You must not share your login with anyone else.
- You should use Microsoft Share Point™ and Microsoft One Drive™ when working with or sharing sensitive data or folders with other Italia Conti employees. You should password protect or encrypt external drives.

[4] https://www.italiaconti.com/policies/

- If sharing information with groups of students, use Microsoft SharePoint™ rather than sending an attachment via email (wherever possible).
- Make sure your devices lock if left inactive for a period of time (automatic screen saver).
- Where possible, avoid sharing devices among family or friends – consider creating separate user profiles if you do need to share a device.
- Install reputable antivirus, anti-spyware and firewall software, e.g., McAfee™, F-Secure™, Norton™.
- Ensure that your computer or device is configured to receive software patches and critical updates. Keep operating systems up to date where possible: this is essential to ensure data security.
- Where possible, activate an ad blocker (this is usually available as part of a good antivirus program).
- You will be expected to undertake the Educare data protection training when requested.
- Please be aware of the *Digital Safety Agreement* (which all students sign) and the *Italia Conti Guidance for delivering online learning* (Staff).
- Networked ICT equipment or computers accessing our networks should only be used in connection with Italia Conti business: use of this ICT equipment (or any other equipment connected to our networks) may be monitored at any time.
- The use of Italia Conti emails and college specific information systems, e.g. Pro-Monitor™, Pro-Solution™ and Aubergine™, plus any facilities provided by partners, e.g. University of East London (UEL), should only be used in connection with official Italia Conti business.
- Do not use memory sticks or other external drives or storage media (DVDs) for storing confidential Italia Conti information. (They can be easily lost!)
- If discussing confidential comments with other staff, consider using a meeting in Microsoft Teams™ to share information, and keep notes centrally on your Microsoft 365™ account. Alternatively, you can create and share a Microsoft Word™ document on Microsoft SharePoint™ for the other members of the team to review and edit.
- Record the details of meetings with students (including comments) using Pro-Monitor™. This is particularly important in connection with meetings relating to attendance or disciplinary issues. If the meeting or comment is about sensitive safeguarding topics, you should use the Confidential Comments feature in Pro-Monitor™.
- Wherever possible store documentation referring to students on their record on Pro-Monitor™.

## Contacting students

When contacting students, please make sure you have hidden your personal number

- On most phones you can hide your number by dialling 141 before making the call (please check your phone's manual to ensure that this feature has been enabled).
- You may find it useful to email a student in advance of calling, so that they accept the call.
- Always use your Italia Conti email address when contacting students or parents.

Use ProMonitor™ to record details if there is a cause for concern.

Make sure your background is appropriate if using Zoom or Teams and add a background if necessary/ possible.

## Special Category data and disposal of confidential data

Special Category data includes information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health (physical or mental), sex life, sexual orientation, and the processing of genetic data, biometric data for the purposes of uniquely identifying a person, e.g. fingerprints, retina and iris patterns.

Personal information should not be kept for longer than is necessary for the purposes for which the data is processed, including for the purpose of satisfying any legal, accounting or reporting requirements.

Any special category or criminal offence data that is disclosed by a student should be noted on ProMonitor™. Sensitive data should be transferred to secure Italia Conti folders e.g. Microsoft One Drive™, and any copies, e.g. deleted promptly. (If possible, use a secure digital shredding option that is sometimes provided as part of your antivirus program, e.g. McAfee Antivirus™.)

Any paper printouts that include confidential data should be securely disposed of, e.g. by shredding.

*hybrid working = when employees can work for all or part of the time from home, and may be using their own personal computers to access Italia Conti computer networks.

## Appendix 4: GDPR Guidelines for Italia Conti staff when working on-site

### Purpose:

To ensure that staff meet key privacy standards whilst using confidential information in the course of their duties.

### Aims:

Italia Conti processes certain personal data about its employees, students and other stakeholders for a variety of specified and lawful purposes; these are identified in Privacy Notices issued to staff, students, alumni and others whose Personal Data it processes.[5] In order to protect the privacy of our stakeholders, and to comply with the principles laid out in law as set out below, Personal Data must be collected and used fairly, stored securely and confidentially, and destroyed when it is no longer needed.

Protecting the confidentiality, integrity and availability of personal data is a critical responsibility that we take seriously at all times. Confidentiality means that only people who have a need to know and are authorised to use Personal Data can access it. Integrity means that the Personal Data we process is suitable for the purpose for which it has been created/obtained. Availability means that authorised users are able to access Personal Data for authorised purposes.

Italia Conti aims to ensure that all Personal Data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and Processed lawfully in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

This policy applies to all Personal Data, regardless of whether it is in paper or electronic format.

It should be read in conjunction with the Data Protection Policy and the Personal Data Breach Guidelines for Staff.

### Procedure (electronic data):

- If using a networked Italia Conti computer, you should only use your own official login to access electronic data and services. You must not share your login with anyone else.
- All emails connected to Italia Conti should be sent from your Italia Conti email address. You should not use your personal email account.
- If bringing your own device to work, you should comply with the official Italia Conti guidelines in force at any given time.
- You should minimise storing Italia Conti data on your personal device(s). This can be achieved by always using your Microsoft Office 365™ login to access and edit documents rather than downloading it to your local machine. Italia Conti provide access to a secure environment via Microsoft One Drive™ and Microsoft Share Point™. Information at setting Microsoft Share Point to automatically use your Microsoft applications on your machine can be found at: https://www.youtube.com/watch?v=hVpX4wQdIhc
- Keep any device you use password protected. Remember that strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers, and special characters (e.g., asterisk or currency symbol).
- You should use Microsoft Share Point™ and Microsoft One Drive™ when working with or sharing sensitive data or folders with other Italia Conti employees. You should password protect or encrypt external drives.

[5] https://www.italiaconti.com/policies/

- If sharing information with groups of students, use Microsoft SharePoint™ rather than sending an attachment via email (wherever possible).
- Make sure your devices lock if left inactive for a period of time (automatic screen saver).
- Where possible, avoid sharing devices among family or friends – consider creating separate user profiles if you do need to share a device.
- Install reputable antivirus, anti-spyware and firewall software, e.g., McAfee™, F-Secure™, Norton™.
- Ensure that your computer or device is configured to receive software patches and critical updates. Keep operating systems up to date where possible: this is essential to ensure data security.
- Where possible, activate an ad blocker (this is usually available as part of a good antivirus program).
- You will be expected to undertake the Educare data protection training when requested.
- Please be aware of the *Digital Safety Agreement* (which all students sign) and the *Italia Conti Guidance for delivering online learning* (Staff)
- Networked ICT equipment or computers accessing our networks should only be used in connection with Italia Conti business: use of this ICT equipment (or any other equipment connected to our networks) may be monitored at any time.
- The use of Italia Conti emails and college specific information systems, e.g. Pro-Monitor™, Pro-Solution™ and Aubergine™, plus any facilities provided by partners, e.g. University of East London (UEL), should only be used in connection with official Italia Conti business.
- Do not use memory sticks or other external drives or storage media (DVDs) for storing confidential Italia Conti information. (They can be easily lost!)
- If discussing confidential comments with other staff, consider using a meeting in Microsoft Teams™ to share information, and keep notes centrally on your Microsoft 365™ account. Alternatively, you can create and share a Microsoft Word™ document on Microsoft SharePoint™ for the other members of the team to review and edit.
- Record the details of meetings with students (including comments) using Pro-Monitor™. This is particularly important in connection with meetings relating to attendance or disciplinary issues. If the meeting or comment is about sensitive safeguarding topics, you should use the Confidential Comments feature in Pro-Monitor™.
- Wherever possible store documentation referring to students on their record on Pro-Monitor™.

## Procedure (office physical security)

- Ensure that confidential paperwork is stored securely and out of sight when not being used.
- Lock office draws and filing cabinets.
- Ensure that offices are locked when unattended.
- Ensure that confidential information is not being displayed on monitors to unauthorised users.
- Ensure that any hard copies that are no longer required are securely shredded using a cross-cut shredder.

## Contacting students

Telephone: when contacting students from Italia Conti premises, please make sure you use official Italia Conti landlines.

Emails: always use your Italia Conti email address when contacting students or parents.

Use ProMonitor™ to record details if there is a cause for concern.

Make sure your background is appropriate if using Zoom or Teams and add a background if necessary/ possible. Wherever possible, always use an official Italia Conti Zoom account when contacting students.

## Special Category data and disposal of confidential data

Special Category data includes information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health (physical or mental), sex life, sexual orientation, and the processing of genetic data, biometric data for the purposes of uniquely identifying a person, e.g. fingerprints, retina and iris patterns.

Personal information should not be kept for longer than is necessary for the purposes for which the data is processed, including for the purpose of satisfying any legal, accounting or reporting requirements.

Any special category or criminal offence data that is disclosed by a student should be noted on ProMonitor™. Sensitive data should be transferred to secure Italia Conti folders e.g. Microsoft One Drive™, and any copies, e.g. deleted promptly. (If possible, use a secure digital shredding option that is sometimes provided as part of your antivirus program, e.g. McAfee Antivirus™.)

Any paper printouts that include confidential data should be securely disposed of, e.g. by cross-cut shredding.

## Appendix 5: Data Protection Impact Assessments (DPIAs)

DPIAs must be conducted when Processing is potentially high risk and the advice of the DPO should be sought. DPIAs should therefore be conducted, and the findings discussed with the DPO when implementing major system or business change programs involving the Processing of Personal Data, including but not limited to:

- use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- automated Processing including profiling and automated decision making;
- large-scale Processing of Special Category Data; and
- large-scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

- a description of the Processing, its purposes and Italia Conti's legitimate interests if appropriate;
- an assessment of the necessity and proportionality of the Processing in relation to its purpose;
- an assessment of the risk to individuals; and
- the measures envisaged to address the risks and to demonstrate compliance with the GDPR.

Note: it is the responsibility of the staff member(s) who are introducing new systems of processing data to draw up the DPIA. The DPO's role is to advise on this process.

## Appendix 6: Guidance for using Emails:

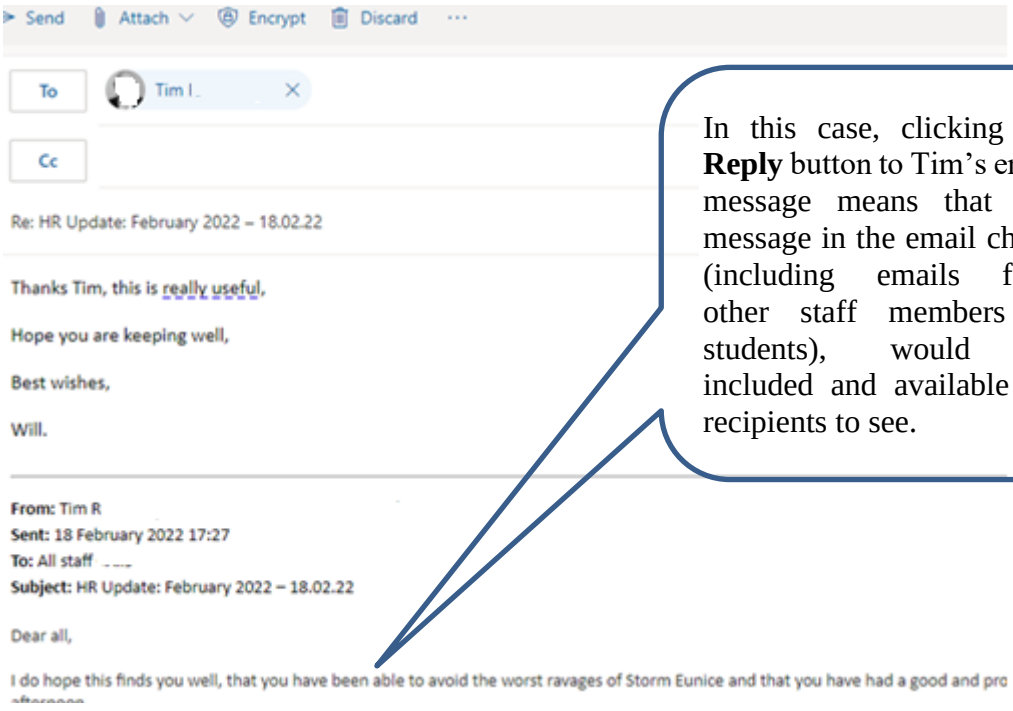
1) Only use your Italia Conti email account for official Italia Conti business.

2) Do not use your official Italia Conti email account for storing or sharing confidential data. (You can use Microsoft SharePoint™ for this instead).

3) When drafting emails, always use courteous and professional language. Remember, under Data Protection laws, students could ask to see copies of any emails sent about them.

4) If you are emailing students, you should only email them on their official Italia Conti student account. (This is important as our IT department is able to see what emails they have seen, and can also delete emails sent to students' accounts in error!)

4) When replying or forwarding emails, always scroll down to check the rest of the email in case there is any sensitive information or comments which you don't want your recipient to see, e.g.



## Sending emails to groups of students (MS Outlook™ web-based version):

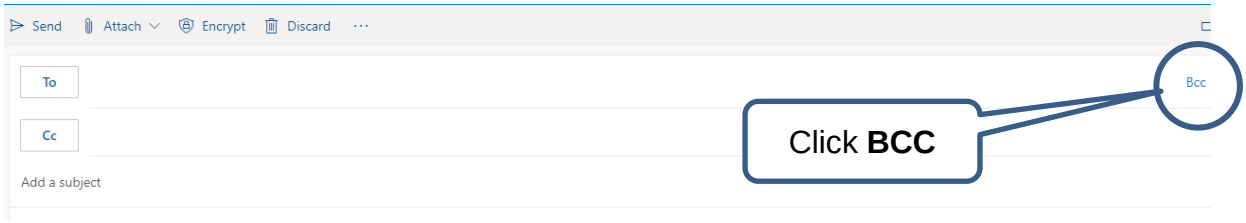
When sending emails to a student or a group of students always follow this procedure:

a) Make sure you are creating a new email. Click the **New message** button in the top left-hand corner of your screen.


**Important**: if you don't click **New Message**, you might inadvertently forward an email which has other emails attached to it which might contain confidential information which you should not share.

b) As you are sending out emails to a group of students, you should select the **BCC** (Blind Carbon Copy) field.
(This prevents the students seeing each other's email addresses, or seeing to whom else the email has been addressed).

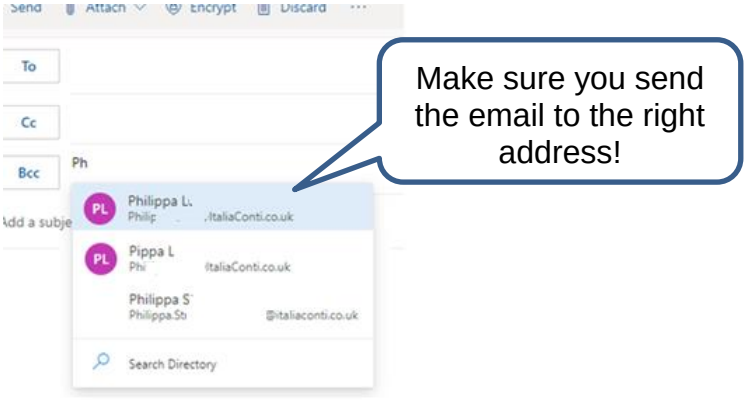
By default, the BCC field always hidden. Click on the **BCC** button the right-hand side of your new email, e.g.




c) You can start to input the email addresses, but always double-check each email address: ask yourself is it the correct one? This is because the email address system uses predictive text that might sometimes give the wrong recipient, e.g. typing in Philippa Luce's email address also brings up a number of others.

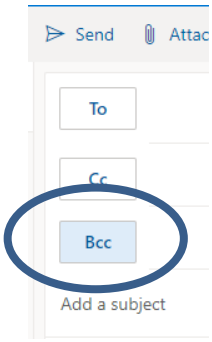
Remember:

It is **easy** to select the wrong recipient.



d) If you are sending the email to a official group of students, it's easier to actually select the group of students from Microsoft Outlook's™ address book. To do so, follow these simple steps:

i) click on the **BCC** button itself, e.g.

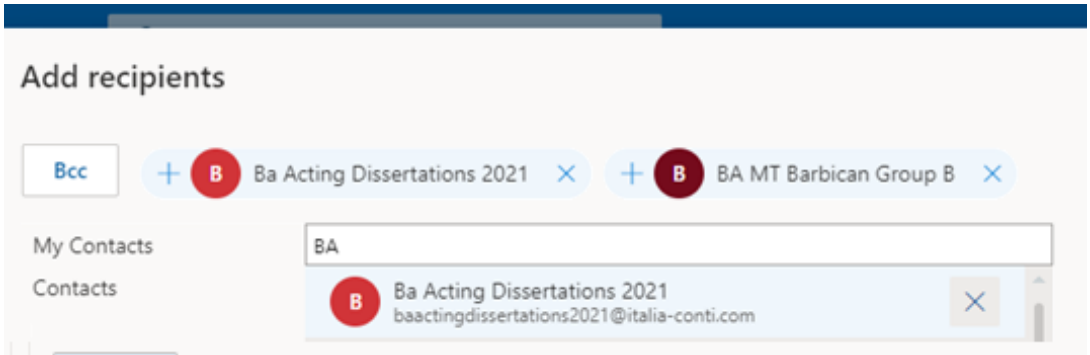



ii) When the **Add Recipients** window appears, click on **Default Global Address List**.

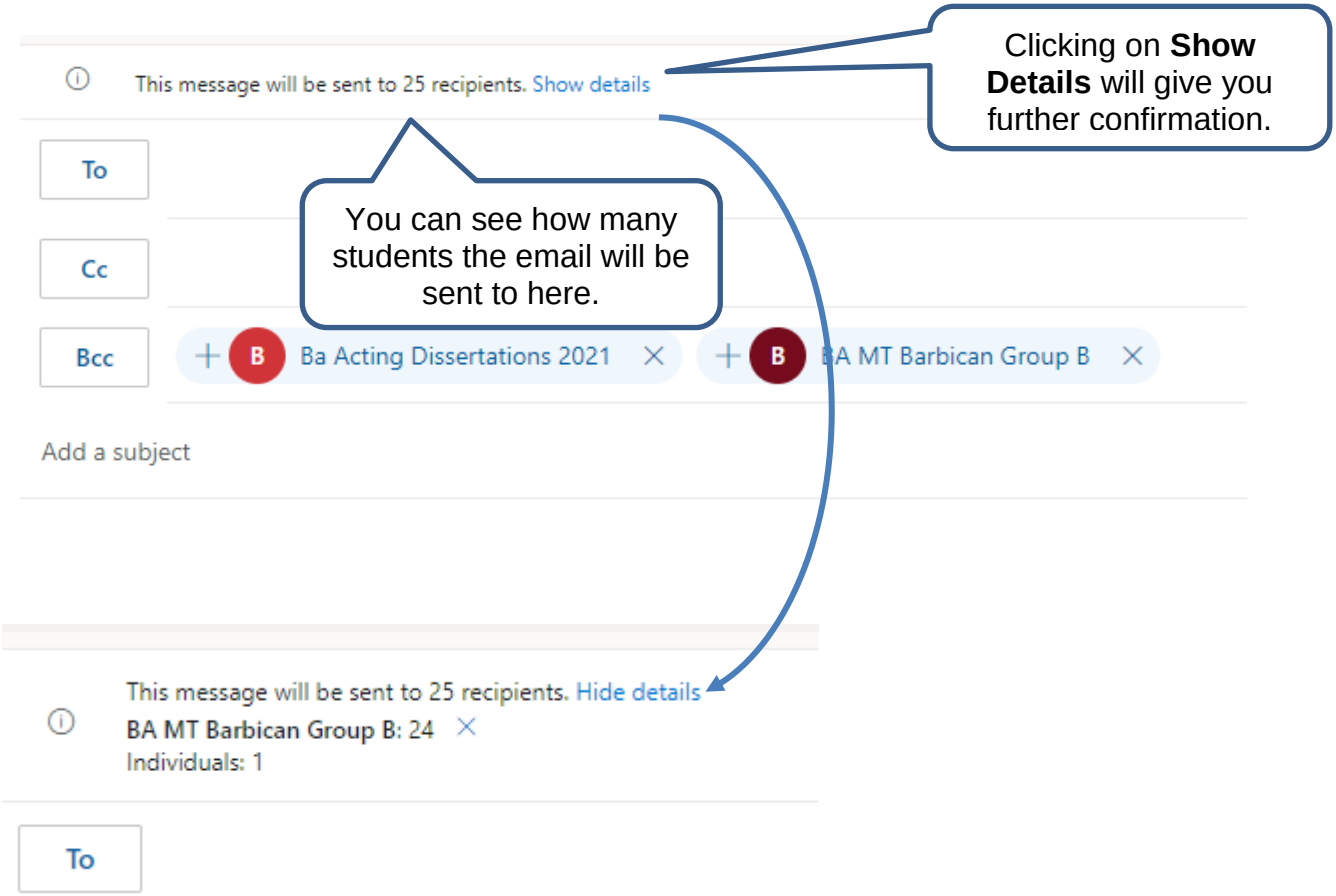
You can then type in the search box a key word in the name of the group(s) you wish to see. In this example, I have done a search for the BA students.


iii) You can scroll through the lists of groups, and can click the **+** button on each one you wish to add.

These are automatically added, e.g.

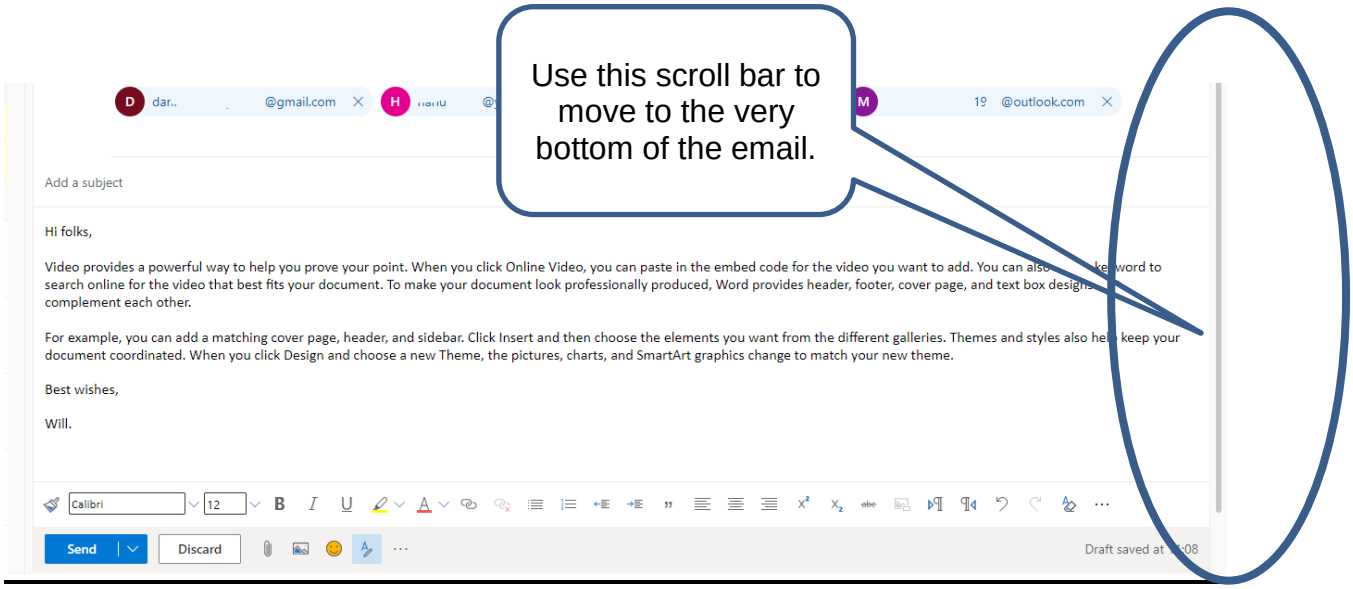


iv) Once you have selected all the groups you need, click the **Save** button in the bottom right-hand corner of the **Add Recipients** window. The email groups will be automatically added to your new email, e.g.




v) If you want to check the individual email addresses in the email, you can click on the + button to expand them, e.g.

vi) Once you have composed your message, proof- read it and make sure you use the right-hand scrolling bar to double-check there is nothing below you new email.




vii) You should then do a final check on the email addresses, and then you can click send.

## Sending documents to students:

Although it is easy to send documents as attachments in Microsoft Outlook™, it is probably safer to use Microsoft Share Point™ for sending files (wherever possible). It will normally tell you when students have accessed the file, and you can remove permissions for people to view files after you have sent the link. (Although this may not help you if they have already viewed the file or have downloaded it to their computer).

a) Information on how to share files using Microsoft SharePoint™ can be found here:

https://www.youtube.com/watch?v=GHzWVjwNH1s (16 mins).

b) Information on removing permissions for students to view files in Microsoft SharePoint™ can be found here:

https://www.youtube.com/watch?v=_hlcRp-cuno (3 mins).

**END**