Data Protection Policy

The Franchisee is responsible for the implementation and oversight of this Policy

Approved by:	Policy Steering Group	Date: 22nd February 2025
Reviewed by:	Data Protection Officer and Head of Quality Assurance	Date: 19th January 2025
Checked by:	Chief Operating Officer	Date: 22nd February 2025
Next review due:		Date: 31st August 2026

This policy will be reviewed by the Policy Steering Group annually unless there are legislative changes

Contents

1) Aims

Italia Conti Associates Franchisees process certain personal data about their employees, students and other stakeholders for a variety of specified and lawful purposes; these are identified in *Privacy Notice*s issued to staff, students, alumni and others whose Personal Data they process.[1] In order to protect the privacy of their 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 Italia Conti Associate Franchisees 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 they 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 Associate Franchisees aim to ensure that all Personal Data collected about staff, pupils, parents, visitors and other individuals is collected, stored and Processed lawfully in accordance with he General Data Protection Regulation (outside UK) 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.

2) Legislation

This policy reflects the requirements of the General Data Protection Regulation (outside UK) 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. The outside UK GDPR was incorporated into UK legislation, with some amendments, by the Data Protection, Privacy and Electronic Communications (Amendments etc) (outside UK Exit) Regulations 2020.

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

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department of Education (DfE) on Generative artificial intelligence in education.

It also reflects the ICO's Code of Practice for the use of surveillance cameras and personal information.

3) Definitions

Accountable Officer (AO): the most senior person in an organisation who has ultimate responsibility for data protection.

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.

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

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.

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

Data Controller: the person/organisation that determines when, why and how to process personal data. For the purpose of this policy, Italia Conti Associates is the Data Controller.

Data Owners: The Franchisees and Italia Conti Associates .

Data Processor: an external person or organisation who Processes information on our behalf, e.g. ThinkSmart Software are the owners of the Dance Biz software which is used for processing our data.

Data Subject: a living, identifiable individual about whom we hold personal data. Data subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

Data Privacy Impact Assessment (DPIA): a tool to identify and reduce the risks of a data processing.

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

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

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

Franchisee: the person who is identified as the Franchise Holder in the Italia Conti Associates' Franchise Agreement.

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.

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.

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. Processing can be automated or manual.

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.

Related Policies: Italia Conti Associates' related policies, guidelines and procedures which assist in implementing this policy are available on our webpage.

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.

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

4) The Data Controller & ICO registration

Italia Conti Associates and Franchisees process personal data relating to parents, pupils, staff, visitors and others, and therefore are Data Controller(s).

Italia Conti Associates is registered with the ICO and has paid its data protection fee to the ICO, as legally required. (Registration Number: ZB089729).

Franchisees of Italia Conti Associates Schools are responsible themselves for registering with the ICO and paying the relevant data protection fee (unless stated in individual terms and conditions).

5) Scope

This policy applies to all staff who must ensure that their Processing of Personal Data on behalf of Franchisees and Italia Conti Associates 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 Overall responsibility

The Franchisee has overall responsibility for ensuring that their respective Italia Conti Associates' School complies with all relevant data protection obligations.

6.2 Data Protection Officer and Accountable Officer

The Data Protection Officer (DPO) for Italia Conti Associates is currently 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.

The Franchisee, as the Accountable Officer, acts as a representative of the Data Controller on a day-to-day basis.

Where relevant, the Accountable Officer will report to Italia Conti Associates for their advice and recommendations on data protection issues.

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

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

6.3 All staff

Staff are responsible for:

- Collecting, storing and Processing any Personal Data in accordance with this policy and data protection law;
- Informing Italia Conti Associates or Franchisees of any changes to their personal data, such as a change of address;
- 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;
    - 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.

7) Core Principles

Italia Conti Associates and Franchisees should ensure that they comply with the following GDPR data protection principles.

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.

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

8) Collecting Personal Data

Franchisees and Italia Conti Associates Processes (e.g., collects and uses) students' Personal Data primarily for the purposes of providing education and training as set out in the *Privacy Notice* for students. Franchisees and Italia Conti Associates also process 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 Notice*s issued. Personal Data should be Processed only for the purposes identified in those *Privacy Notice*s

8.1 Lawfulness, fairness and transparency

Franchisees and Italia Conti Associates will only process personal data where we have 1 of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The Personal Data needs to be Processed so that Franchisees and Italia Conti Associates can **fulfil a contract** with the individual, or the individual has asked Italia Conti Associates to take specific steps before entering into a contract;
- The Personal Data needs to be Processed so that Franchisees and Italia Conti Associates **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 Franchisees and Italia Conti Associates 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**.

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

- 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;
- 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 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

  Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) 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.

8.2 Limitation, minimisation and accuracy

Franchisees and Italia Conti Associates will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals 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 collect 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.

9) Sharing personal data

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).
    - Italia Conti Associates 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.

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.[2] 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 Franchisees and Italia Conti Associates with a legal basis for supplying the data under the DPA exemptions.

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

If a non-standard application is made, then Franchisees and Italia Conti Associates 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.

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

Franchisees and Italia Conti Associates 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.

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;
- 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.

10) Subject access requests and other rights of individuals

10.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that Italia Conti Associates holds about them. 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 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.

Subject access requests can be submitted in any form, but Italia Conti Associates 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

To make a 'subject access request', contact Italia Conti Associates at dpo@italiaconti.co.uk.

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

10.2 Children and subject access requests

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.

Children below the age of 12 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 Associates 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.

Children aged 12 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 12 and over at Italia Conti Associates 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.

10.3 Responding to subject access requests

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.

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

- might
- 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.

If the request is 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.

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.

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

10.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their 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).

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.

11) Parental requests to see the educational record[3]

Parents, or those with parental responsibility, have a right to access their child's educational records.

12) Biometric recognition systems

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

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.

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 Associates will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

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

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

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).

Where staff members or other adults use the Italia Conti Associates' 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 Franchisee and Italia Conti Associates will delete any relevant data already captured.

13) CCTV

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

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.

Any enquiries about the CCTV system should be directed to the owner of the premises upon which it is operating.

14) Photographs and videos

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

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.

Italia Conti Associates' Franchisees 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.

Any photographs and videos taken by parents/carers at Italia Conti Associates 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.

Where Franchisees and Italia Conti Associates takes photographs and videos, uses may include:

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

Consent can be refused or withdrawn at any time. If consent is withdrawn, Franchisees and Italia Conti Associates will take reasonable steps to delete the photograph or video and not distribute it further.

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.

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

15) Artificial Intelligence

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, students, and parents/carers may be familiar with generative chatbots such as ChatGPT™ and GoogleBard™. Italia Conti recognises that AI has many uses to help students learn, but also poses risks to sensitive and Personal Data.

To ensure that Personal and sensitive Data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If Personal and/or sensitive Data is entered into an unauthorised generative AI tool, Italia Conti will treat this as a data breach, and will follow the Personal Data breach procedure outlined in **Appendix 1**.

16) Data protection by design and default

Franchisees and Italia Conti Associates 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 Franchisees and Italia Conti Associates' 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 Notice*s
- 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 Associates and DPO and all information we are required to share about how we use and process their personal data (via our *Privacy Notice*s)
    - 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 UK and the safeguards for those, retention periods and how we are keeping the data secure.

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 Associates, by taking appropriate steps to maintain security of personal data. Staff should therefore follow all procedures and use the technologies Italia Conti Associates 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.

Further information can be found in **Appendix 3: GDPR Guidelines for Italia Conti Associates' staff when working from home**.

17) Storage Limitation

Franchisees and Italia Conti Associates 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.

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.

Franchisees and Italia Conti Associates 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.

18) Disposal of records

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.

For example, we 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 Associates' behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

19) Personal data breaches

Franchisees and Italia Conti Associates will make all reasonable endeavours to ensure that there are no personal data breaches.

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

When appropriate, Franchisees and Italia Conti Associates will report the 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 school laptop containing non-encrypted personal data about students; or
- 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.

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 Associates' staff when working from home.**

Actions to minimise the impact of Personal Data Breaches

Italia Conti Associates 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.

Data breach helpline:

Italia Conti Associates 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 of our Cyber Insurance policy.

Please note: this helpline should only be used by the DPO where it is suspected that a breach might lead to a claim.

20) Training

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

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Italia Conti Associates' processes make it necessary. Staff knowledge of the Data protection procedures will be refreshed annually. Training will also be offered to established Associate Schools retrospectively.

21) Monitoring arrangements

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

This policy will be reviewed **annually** and shared with the Senior Leadership Team.

22) Links with other policies

This data protection policy is linked to our:

Privacy Notices

Safeguarding & Child Protection Policy

Social Media Policy

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.
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 Associates . 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 Italia Conti Associates' Franchisee. (If the breach is not deemed serious, the Italia Conti Associates' Franchisee 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 Italia Conti Associates' School's *GDPR Incident Log*.
5) Review the data breach incident as part of the normal review process with Italia Conti Associates 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 Italia Conti Associates' Franchisees will meet as soon as possible to review what happened, and how it can be stopped from happening again. (This may be an online event).

Data breach helpline:

Italia Conti Associates 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 staff working from home

Purpose:

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

Aims:

Franchisees and Italia Conti Associates process certain personal data about its employees, students and other stakeholders for a variety of specified and lawful purposes; these are identified in *Privacy Notice*s 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.

Franchisees and Italia Conti Associates 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:

- All emails connected to Italia Conti Associates should be sent from your official Italia Conti Associate email address.
- You should not use your personal email account. You should minimise storing Italia Conti Associates' data on your personal device(s). 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).

- 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 and anti-spyware 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 data protection training when requested.

[4] https://www.italiaconti.com/about-us/policies

- Please be aware of the *Digital Safety Agreement* (which all students sign) and the *Italia Conti Guidance for delivering online learning* (Staff)

Contacting students

When contacting students by telephone, 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 Associate email address when contacting students or parents.
- 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 paper printouts that include confidential data should be securely disposed of, e.g. by shredding.

Appendix 4: 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 Associates' 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. Advice can be provided by contacting the Italia Conti DPO at dpo@italiaconti.co.uk

A standard DPIA template provided by the Information Commissioner's Office is available on the next page.

Sample DPIA template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and you should read it alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

Start to fill out the template at the beginning of any major project involving the use of personal data, or if you are making a significant change to an existing process. Integrate the final outcomes back into your project plan.

Step 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated, reduced or accepted	Low, medium or high	Yes/no

Step 7: Sign off and record outcomes

Item	**Name/date**	**Notes**
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons

Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA

END