info@my360plus.com

Contents

Executive Summary

Part One: Public Documents

Materials are publicly available, found on the my360plus website and are linked to relevant emails to Customers, Administrators, Participants, and Observers.

Part Two: Policy Documents

These documents form an integral part of our internal processes and are regularly reviewed.

Part One: Public Documents

The following materials are found on the my360plus website and are linked to relevant emails to Customers, Administrators, Participants, and Observers.

GDPR and Data Protection

For privacy, data protection and GDPR reasons, my360plus follows strict security procedures in the storage and disclosure of personal data, to prevent unauthorised access.

This is in accordance with data protection legislation in the UK, EU and elsewhere.

How we manage feedback and personal data

Overview - Participant and Observer - Definitions

- If you are a subject (**Participant**) completing a my360plus assessment, we will process personal data from you and your Observers, in order to create a report.
- If you are an **Observer** of a Participant (the subject of a my360plus assessment), your email is used in order to send you a link to the my360plus survey questionnaire and, if you further consent, automated emails regarding ongoing feedback, linked to the Participant's Personal Development Plan (PDP).

Some people may be both Participants **and** Observers.

- **Customers** of my360plus are typically end-user organisations or specialist HR/ L&D suppliers to end users.
- Customers may appoint **Administrators** to manage their my360plus programme, which may give them access to data and a participant dashboard.
- It is the Customer's responsibility to ensure data protection of their Participants and Observers by their Administrators.

Permissions

If you are undertaking a my360plus assessment with your employer, then, by submitting this information you grant us the right to share this information with your employer.

We do not sell, rent or exchange personal information with any other third party for any reason.

Contact details

My360plus is owned by the Forton Group Ltd, registered with the ICO under registration reference Z6898165

Registered Office: College Farm, Main Street, Willoughby, Rugby, Warwickshire, CV23 8BH, United Kingdom

For all GDPR enquiries info at my360plus dot com') marked "GDPR"

We support both the spirit and letter of the GDPR.

The Forton Group Ltd is registered with the ICO under registration reference Z6898165; see https://ico.org.uk/ for details about ICO.

DATA held for the purposes of delivering my360plus services

Our lawful basis for holding data is for the purposes of enquiries, education, and training, and for the my360plus service, which is a minimum one year subscription service enabling access to the my360plus platform, with the option to extend for a second year.

Enquiries: Product and Service Information Provision.

We provide information in response to enquiries from organisations or members of the public using the following data:

- Name/surname
- Job title
- Organisation
- Email
- Phone
- Address (if printed material requested)
- Education and training – we hold the following student data
    - Name/surname
    - Job title
    - Organisation
    - Email
    - Phone

Address (if printed material requested)

Specifically, for Chartered Management Institute (CMI) educational requirements, we may additionally hold the following data

- Date of Birth
- Professional body registrant or membership number (e.g. GDC)

Specifically, for International Coach Federation (ICF) educational and accreditation requirements, we may pass relevant data outside the EU (to the UK and USA).

- Users of the Forton Group online learning management system (LMS) are registered on the 'Full Partner' LMS. Their name and email data (accessible via password) will be held outside the EU (UK and USA). LMS users control their own passwords, so that they can use the LMS system.
- Educational data must be held for up to three years, so that record keeping and verification may be used to achieve professional qualifications.

The my360plus online survey system collects three types of data:

- Customer administration data for dashboard access
- Participant data
- Observer data

GDPR and data protection

Control and removal

Administration and Participants control their username and email address under password, so that they can access the dashboard (Administrators), their subscription (Participants) and reports.

- Administrators can be removed at any time and should be removed on change of role
- Data from enquiries or information provision can be removed at any time.
- Participant personal data can be removed 1 year after completion of the annual subscription, or renewed, or on request.
- Observer personal data is linked to Participants and can be removed 1 year after completion of the annual subscription, or renewed, or on request.
- Student data can be removed after 3 years.

Storage and sharing

We have documented what personal data we hold, where it came from, who we share it with and what we do with it. We store data through third party suppliers in these ways:

- Mailing systems: Lifeboat marketing and Outlook
- Secure data and file storage backup/security system (Dropbox)
- Learning Management Systems (Full Partner)
- Live Virtual Classroom Service (Zoom)
- Conference Calling service (Powwownow)

We have written agreements with suppliers to secure your data. We have compliance processes in the event of a security breach. This includes the security of personal data processed by others on our behalf that is transferred outside the European Economic Area (e.g. cloud storage).

Right of access & right to object

You can access the data/ information we hold on you by providing

- a valid email address
- proof of name
- sent to the contact details 'info at my360plus dot com'

We will respond within 14 days. Part of our process is to check the validity of the name/email given prior to responding.

Current Registered Students, Administrators and Participants can update their own data, using their Username and Password.

You have the right to object to our holding data.

Privacy notice

For all GDPR enquiries contact info [at] my360plus [dot]com

- The Lead Data Protection Officer and Controller is Helen Caton-Hughes, Managing Director. Email: Helen dot Caton [at] thefortongroup [dot] com
- We train all Staff, Faculty Members, Partners and Associates in our policies and in the GDPR requirements, in order to provide the best possible service using the minimum personal data.
- Our non-EU regional Directors also receive training in the GDPR and data protection requirements.
- Your right to rectification If your data is incorrect, we will update it within 14 days of notice.
- We will contact you annually to confirm your data is correct and that (in the case of information provision) you wish to remain on our database.
- For students, we will contact you at the end of 3 years from the start date of your education programme to check whether you wish to remain on the database.

We inform customers and partners who register clients or staff members for the purpose of using the my360plus services of the following statement:

> "For development purposes (using the my360plus system) we will keep participant and observer records for a minimum of one year (the standard my360plus subscription term) and after that for the purpose of renewing the subscription at the request of the Customer or Partner. We keep the minimum possible data. After this point, personal data is removed and remaining data used for the purpose of anonymous verification of the my360plus benchmarking data."

We inform individual or corporate customers who train staff members of the following statement:

> "For educational purposes (leadership development and/or coaching) we will keep student records for a minimum of three years and after that for the purposes of providing proof of attendance/completion to the student (e.g. for attendance dates/lost certificates/letters etc) or at the request of ICF/CMI or other accrediting bodies. We supply the minimum possible data. Students can opt out at any time, on the understanding that the Forton Group will be unable to provide attendance evidence once the student has opted out."

Data Transfer

The one piece of documentation in the my360plus system which is 'transferable' is the pdf version of the Participant's Report. This is identified only by the given name of the Participant. There is no other personal identifying data in the report.

At the request of the Customer, the Administrator or the Participant, this data may be transferred internationally. Once downloaded by any of these, it's transfer is outside the control of my360plus.

Safeguards

Safeguards are in place to keep personal data stored securely on encrypted systems for back-up and security purposes.

Procedures for security incidents, and responses to incidents are in place.

Secure disposal

We make all reasonable efforts to dispose of data safely.

Your right to restrict access

You have a right to expect us to restrict access to your data for the purposes you choose, so that you can maintain optimum privacy.

We offer the following restrictions:

- Registered Participant
- Student
- Psychometric tools – User, Observer or Rater
- Corporate client
- Coach
- my360plus reports, for individuals and teams
- Other educational materials or courses (video, audio, written)
- Information

Opt-in

You can opt-in or out of receiving information, which includes details of the following types of products and services offered:

Leadership • Coaching & Mentoring • Psychometric tools (e.g. my360plus) • Accredited qualification programmes • ELearning Student

Legitimate Interest Assessment and Statement

The Forton Group provides research, education, leadership development and coaching services. We operate through a range of brands and companies, for the purposes of individual leadership and management development, and for team development:

Forton Group Companies

- The Forton Group Limited
- The Leadership Coach Limited
- Dental Coaching Academy Limited
- The Forton Group OÜ

Brands/websites

- The Forton Group
- My360plus
- Professional Leadership Coaching
- Dental Education Centre
- Igniting Excellence in leadership

What is Forton's "Legitimate Interest"?

The Forton Group is an educational organisation which specialises in leadership development and coaching, so that organisations are more successful, and leaders and managers feel more fulfilled.

The International Coach Federation and the (UK) Chartered Management Institute accredits the Forton Group for the purpose of awarding professional qualifications.

The Forton Group registers my360plus participants and observers, and training course participants ('students'), so that they can learn and develop professionally, through in-person and virtual (digital) methods, receiving feedback reports, accessing reading, audio and visual materials.

Information about these services is available to anyone who completes either a contact form on the my360plus.com website or requests a product demonstration. These contact details are stored for the purposes of providing the product/service information or the demonstration. A link to the privacy policy is available at the time of providing contact details.

Definitions

These are the definitions we use to describe who is registered on the system, and by whom

- A Participant – by their employer for the purpose of undertaking a self-assessment and receiving online 360 degree feedback from observers.
- An Observer – by their employer, or by a colleague, for the purpose of giving online 360 degree feedback to participants.
- An Administrator – registered with the permission of their employer, so that they can administer the my360plus dashboard on behalf of their employer.
- A Partner is a customer of my360plus, for the purpose of acting as supplier to an end-user client of the my360plus service.
- A Partner may also be an Administrator for the purpose of managing the my360plus dashboard.
- A Student is someone who registers for some educational material themselves, or by their employer for the purpose of accessing the LMS.

Participants, Observers, Partners, Students and Administrators are registered via email, websites, the my360plus system and the Forton Learning Management System (LMS), so that they can access and use the system.

Why data processing is necessary to deliver the service

Personal data is necessary to:

- Prepare the report. E.g. email instructions, reminders or development goals to Participants and/or Observers.
- Maintain the dashboard records, so that Administrators can track progress.
- Communicate between the Partner and/or Customer and my360plus, so that any issues are addressed.
- Email any written educational material, logistics information (e.g. date/time of event, location, access passwords etc)

- Use Username and Passwords, in order to to access student-only learning materials
- Keep records in order to produce certificates and inform any relevant accrediting bodies

Forton balances this need against the individual's interests, rights and freedoms, in order to provide the services, as follows:

- Keep minimum data necessary (usually name, email, phone number, and address if printed materials are sent by post), in order to use the relevant service.
- Keep any additional data only if required by an accrediting or professional body (e.g. date of birth (CMI) or professional registrant number (GDC)
- Students/Participants/Observers/Administrators can opt out at any time, on the understanding that the Forton Group will be unable to provide materials or evidence once the person has opted out.

GDPR and data protection consent

Consent is not a pre-condition of a service. However, withholding or removal of consent does have practical implications. EG the Forton Group will be unable to provide logistical information, participant reports, educational services or attendance evidence once a relevant person has opted out.

If you have any questions about privacy please email info@my360plus.com.

Part Two: Policy Documents

The following documents form an integral part of our internal processes and are regularly reviewed.

Appendix 1

Information security and privacy policy

My360plus is the online 360 feedback tool that identifies your peoples' leadership qualities, creates development goals, engages a peer-coaching network and measures progress.

If you are a subject (Participant) completing a my360plus assessment, we will process personal data from you and your Observers, in order to create a report.

This policy will apply in all locations where we operate to all forms of information and to all systems used to collect, store, process or transfer information.

My360plus applies the UK Data Protection Act 2018 as a global privacy standard together with local data protection law in the countries where it operates. In

countries where the UK Data Protection Act 2018 conflicts with local law, local law that meets internationally accepted privacy principles will take precedence.

My360plus is committed to:

- protecting the confidentiality, integrity and availability of the information it collects, stores, transfers and processes in accordance with UK law and international good practice, and to meeting its legal requirements and contractual obligations
- explaining why it needs personal information, only asking for the personal information it needs and only sharing personal information within My360plus and with other organisations as necessary or where the person concerned has given their consent
- allowing people to request access to the personal information it holds on them and to complain if they believe their information has been mishandled
- not keeping personal information for longer than necessary
- taking measures to protect the rights and freedoms of individuals whose personal information may be transferred to countries with differing data protection laws
- ensuring that actual or suspected breaches of information security are reported and investigated
- assessing and measuring the maturity of its information security controls annually
- applying these standards to its supply chain and delivery partners.

We will provide adequate and appropriate resources to implement this policy and will ensure it is communicated and understood.

My360plus will review this global policy statement annually to reflect new legal and regulatory developments and ensure good practice.

Appendix II

Data Backup Policy

Scope

The service and hence this policy has been designed and implemented with disaster recovery/business continuity (i.e. the ability to recover recent live data in the event of a partial or total loss of data) as key deliverable and is not therefore designed as a method of archiving material for extended periods of time.

The 'data' backups cover all systems managed by My360plus. All individuals are reminded that they are individually responsible for data held locally on their desktop or laptop computer and all critical data *must* be stored on the network drives provided or central e– mail services.

Backup Policy

- Full backups of all My360plus data are performed weekly. Full backups are retained for 3 months before being overwritten.
- Incremental backups of all My360plus data are performed daily. Incremental backups are retained for 1 month before being overwritten.
- Where possible backups are run overnight and are completed before 8am (UTC) on working days.
- Backups are stored in secure locations. A limited number of authorised personnel have access to the backup application and media copies.
- Backups are replicated in at least 2 different secure locations.

- Requests for backup data from 3rd parties must be approved by the Information Security Manager.
- Backup of data held within Database Systems have data backup routines which ensure database integrity is retained. Currently this means systems are not needed to be taken off–line in order to backup.
- Any failed backups are re–run immediately the next working day.
- Data is available for restore within a few minutes of a backup job completing on the daily schedule.
- Data will be available during the retention policy of each backup job – which is currently defined as 3 months.
- Requests for data recovery should be submitted to the IT Service desk.

This policy will be reviewed on an annual basis and be tabled for approval with My360plus directors.

Appendix III

Information Classification Policy

This policy outlines the information classification scheme we have in place as well as our information handling standards. The aim of the policy is to ensure that information is appropriately protected from loss, unauthorised access or disclosure.

Scope

This policy applies to all of the information owned and handled by My360plus, irrespective of the data location or the device it resides on. It should be used by all My360plus employees, including any third party working on the organisation's behalf.

Standards

Information Classification Scheme

Our information classification scheme has three categories: **PUBLIC**, **INTERNAL USE** and **CONFIDENTIAL**.

The levels of classification are summarised in the table below:

Level	Confidentiality	Integrity	Availability
0	PUBLIC	Low	Low
1	INTERNAL USE	Medium	Medium
2	CONFIDENTIAL	High	High

Access to, and use of, LEVEL 2 (Confidential) information is restricted to authorised users with an immediate need to know; and then only for so long as that need exists and only to the extent of that need. Information classified as LEVEL 2 (Confidential) must be subject to protection at all times.

When exchanging data with other organisations or third parties which has been classified/labelled, recipients should ensure that conflicts of variances in classification systems are resolved. Data imported into My360plus systems should be annotated with the approved organisational classification and any conflicting labelling by the originator should be removed.

Documents marked 'Public' may not be re-classified to any other level. Documents in the two other levels are likely, over time, to move into the 'Public' classification.

Integrity

Value of the integrity of information should be assessed as follows:

Integrity Value	Low	Medium	High
Description	Negligible or low impact arising from a breach in integrity	Moderate impact arising from a breach in integrity	High impact arising from a breach in integrity

Examples	Generic system text / content	Observer comments	Participant data / reports

Availability

The availability value of information should be based upon the impact of any period of partial or full unavailability:

Availability Value	**Low**	**Medium**	**High**
Description	Information where the owner is prepared to accept a medium to long term loss of availability of information/service	Information where the owner is prepared to accept a short to medium term loss of availability of information/service	Information where the service is critical and absolutely minimal loss of availability of information/ service is acceptable
Examples	Generic system text / content	Observer comments	Participant data / reports

Responsibilities

The Chief Information Officer is the designated owner of this policy on behalf of the Executive Leadership Team.

Document Authors are responsible for assigning a classification category to the documents they create and protectively marking the document.

All My360plus staff are responsible for protecting information in accordance with this Policy and for meeting the standards set within it. They must respect the security classification of any information as defined. All data breaches should be reported.

Appendix IV

Information Risk Management

Purpose

Information that is collected, analysed, stored, communicated and reported upon may be subject to theft, misuse, loss and corruption.

However, the implementation of controls to protect information must be based on an assessment of the risk posed to the organisation and must balance the likelihood of negative business impact against the resources required to implement the controls, and any unintended negative implications of the controls.

This policy sets out the principles that My360plus uses to identify, assess and manage information risk, in order to support the achievement of its planned objectives, and aligns with the overall organisations risk management framework and approach.

This high-level Information Risk Management Policy sits alongside the Information Security Policy and Data Protection Policy to provide the high-level outline of and justification for the My360plus risk-based information security controls.

Objectives

The My360plus information risk management objectives are that:

- Our information risks are identified, managed and treated according to an agreed risk tolerance
- Our physical, procedural and technical controls are agreed by the information asset owner
- Our physical, procedural and technical controls balance user experience and security
- Our physical, procedural and technical controls are cost-effective and proportionate.

Scope

The Information Risk Management Policy and its supporting controls, processes and procedures apply to all information used at My360Plus, in all formats.

The Information Risk Management Policy and its supporting controls, processes and procedures apply to all individuals who have access to My360plus information and technologies.

A detailed scope, including a breakdown of users, information assets and information processing systems, is included in the Information Security Management System (ISMS) Framework document.

Compliance

Compliance with the controls in this policy will be monitored by the Information Security Manager and reported to the directors.

Review

A review of this policy will be undertaken by the Information Security Manager annually or more frequently as required and will be approved by the directors.

Policy Statement

Information Risk Assessment is a formal and repeatable method for identifying the risks facing an information asset. It is used to determine their impact and identify and apply controls that are appropriate and justified by the risks.

It is My360plus' policy to ensure that information is protected from a loss of:

- Confidentiality – information will be accessible only to authorised individuals
- Integrity – the accuracy and completeness of information will be maintained
- Availability – information will be accessible to authorised users and processes when required

1. Risk assessment

Risk assessments must be completed with access to and an understanding of:

- My360plus' business processes
- The impact to the organisation of risks to business assets
- The technical systems in place supporting the business
- The legislation to which My360plus is subject
- Up-to-date threat and vulnerability assessments

A risk assessment exercise must be completed at least:

- For every new information-processing system
- Following modification to systems or processes which could change the threats or vulnerabilities
- Following the introduction of a new information asset
- When there has been no review in the previous three years

2. Threats

My360plus will consider all potential threats applicable to a particular system, whether natural or human, accidental or malicious.

My360plus will reference Annex C of the ISO 27005 standard to aid with threat identification.

Threat information will be obtained from specialist security consultancies, local and national law enforcement agencies and security services, and contacts across the sector and region.

It is the responsibility of the Information Security Manager to maintain channels of communication with appropriate specialist organisations.

3. Vulnerabilities

My360plus will consider all potential vulnerabilities applicable to a particular system, whether intrinsic or extrinsic.

Vulnerability information will be obtained from specialist security consultancies, local and national law enforcement agencies and security services, technology providers and contacts across the sector and region.

It is the responsibility of the Information Security Manager to maintain channels of communication with appropriate specialist organisations.

4. Risk Register

The calculations listed in the risk assessment process will form the basis of a risk register.

All risks will be assigned an owner and a review date.

5. Risk Treatment

The risk register will include a risk treatment decision. The action will fall into at least one of the following categories:

- Tolerate the risk – where the risk is already below the organisation's risk appetite and further treatment is not proportionate
- Treat the risk – where the risk is above the organisation's risk appetite, but treatment is proportionate; or where the treatment is so simple and cost effective that it is proportionate to treat the risk even though it falls below the organisation's risk appetite
- Transfer the risk – where the risk cannot be brought below the organisation's risk appetite with proportionate treatment, but a cost-effective option is available to transfer the risk to a third party
- Terminate the risk – where the risk cannot be brought below the organisation's risk appetite with proportionate effort/resource and no cost-effective transfer is available

The Information Security Manager in collaboration with the Information Asset Owner will review Medium and Low risks and recommend suitable action.

The directors in collaboration with the Information Asset Owner will review High risks and recommend suitable action.

In the event that the decision is to Treat, then additional activities or controls will be implemented via a Risk Treatment Plan.

6. Roles and Responsibilities

The Information Security Manager has accountability to the directors for managing information risk.

They will direct the information risk appetite for the organisation and review the information risk register. They will be involved in assessing and reviewing High risks.

The Information Security Manager will conduct risk assessments and recommend action for Medium and Low risks, where these can be clearly defined in terms of the organisation's risk appetite.

Information Asset Owners must be responsible for agreeing and implementing appropriate treatments to risks under their control. They must also take an active role in identifying and reporting new risks.

7. Risk Appetite and Tolerance

My360plus has agreed a series of risk appetite statements.

While not exhaustive, these give a good overview of the organisation's desire to pursue or tolerate risk in pursuit of its business objectives.

Appendix V

Media Handling and Transport Policy

Scope

This policy sets out the way in which personal or sensitive data must be transferred by or on behalf of My360plus, whether it is held on paper or electronically. The policy is applicable to My360plus employees, contractors, services providers and other organisations or agencies working for or on behalf of the organization.

Identifying Personal Data

Personal data includes any data that relates to a living individual, or which could identify an individual. It can also include any contextual data about individuals that

when combined with other data will identify an individual. Personal data also includes any expression of opinion about the individual, or any other person, in respect of that individual. This could include letters, correspondence or spreadsheets that contain the names or other data in regard to My360plus', customers, clients or staff.

Personal Data Must Be Electronic Wherever Possible

Data that is transferred between different areas of the business, should be carried out electronically by default wherever possible.

Email will be considered secure within the My360plus network

Emails that are sent within the My360plus network are considered secure.

Data sharing within My360plus

Where there is a business need, and where it is necessary and appropriate, data will be shared between service areas. Only the necessary amount of data will be shared.

Employees should not email sensitive documents unless necessary. Instead references to 'source records' should be used where possible. This means that data is stored in one secure, primary location and those staff who require access to it are given access in a controlled manner.