DATA PROTECTION AND ACCEPTABLE USE OF IT POLICY

1. INTRODUCTION

Athena Global Education (AGE) is required by law to comply with the Data Protection Act 2018 and is committed to ensuring that every current employee and registered student complies with this Act regarding the confidentiality of any personal data held by the College in whatever medium.

The College needs to keep and process certain information about its past, current and potential employees and students to allow it to function effectively and to monitor performance and achievements. To comply with the law, information must be collected, shared, and used fairly, stored safely and not disclosed to any other person unlawfully. A key part of the 2018 Act was the new General Data Protection Regulations (GDPR), which came into effect on 25 May 2018 and applies to all organisations, including charities and voluntary organisations, that process personal data.

Data held and processed on past, present and future students may include personal information, assessment information; and financial information. The 2018 Act notes that 'If your organisation holds personal data, whether in the form of contact information or any other sorts of personal data (for example, information about ethnicity, religious belief, or bank account or credit card information) elements of the new regulations apply to you' So the College has specific responsibility for all its learner data.

In framing this Policy, the College recognises the key Data Protection Principles:

1. Personal data shall be processed fairly and lawfully and shall not be processed unless certain conditions are met.
2. Personal data should be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose.
4. Personal data shall be accurate and where necessary kept up to date.
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data (data relating to a living individual who can be identified) shall be processed in accordance with the rights of data subjects under the Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

2. STUDENTS ARE RESPONSIBLE FOR

- ensuring that all personal data provided to the College is accurate and up to date;
- informing the Student Office of any changes to information which they have provided, e.g. change of address;
- informing the Student Office of any errors or changes.

Students should ensure that they are familiar with the Data Protection Policy. Any breach of the Policy, whether deliberate or through negligence, may lead to disciplinary action being taken, access to the College facilities being withdrawn, or even a criminal prosecution.

3. THE MANAGEMENT OF CONFIDENTIAL INFORMATION

3.1 Scope

This document sets out the College Data Protection Policy aimed at ensuring that the processing and use of personal data held by the College is in accord with the data protection (GDPR) principles within the 2018 Act. The quantity of data processed by the College means it does not need to appoint a Data Protection Officer. The eight principles of Data Protection established by the 1998 Act remain unchanged. Notable that data should be:

Fair and Lawful;

Specific for its purpose;

Adequate and only for what is needed:

Accurate and up to date;

Not kept longer that is needed;

Take into account people's rights;

Kept safe and secure;

Not transferred outside the EEA.

This Policy accommodates these eight principles.

3.2 Disclosures

Within the College, personal data must only be shared with other staff who need it in order to do their work. Personal data must be accessed for work purposes only and not used for any personal purposes.

3.3 Identity Verification

Before making changes or releasing detail of personal records the identity of the requester must be confirmed in order to avoid malicious or fraudulent claims. This process will involve the presentation of original photographic (passport, driving license, etc.) evidence.

3.4 Responsibility for implementation

The Head of Operations is responsible for the implementation of this Policy; compliance with the Policy is compulsory for all staff and students connected with the College.

4. FREEDOM OF INFORMATION

The College acknowledges its responsibilities under the UK Freedom of Information Act. It will acknowledge any written request for information and inform the applicant whether they 'hold any information falling within the scope of their request' (QAA). They will then respond, within 20 working days, by providing that information.

5. PROCEDURES FOR COMPLAINTS

If an individual makes a complaint or is otherwise dissatisfied with the way their personal information is being processed by the College, they should contact the Course Leader.

6. RESPONSIBILITIES OF STAFF

All staff are responsible for:

- checking that any data that they provide to the College in connection with their employment is accurate and up-to-date;
- informing the College of any changes to this data e.g. change of address;
- checking the data that the College will send out from time to time giving details of information kept and processed about them, and informing the College of any errors.

Staff collect data about other people (e.g. about student's course work, opinions about ability, references from other academic institutions, or details of personal circumstances).

Any member of staff who considers that the Policy has not been followed in respect of personal data held, should raise the matter initially with the Course Leader.

7. DATA SECURITY

All staff are responsible for ensuring that any personal data which they hold is kept securely. In addition, personal data is not disclosed to any unauthorised third party either orally or in writing.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases. Personal data is all computerised.

8. STUDENT OBLIGATIONS: STUDENT ENGAGEMENT IN LEARNING

Students must ensure that all personal data provided to the College is accurate and up-to-date. They must ensure that changes of address etc. are notified to the College as soon as possible.

9. RIGHTS TO ACCESS DATA

Staff, students and other users of the College have the right to access any personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should make a request to the Course Leader.

The College aims to comply with requests for access to personal data as quickly as possible, but will ensure that it is provided within 21 days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the person making the request.

10. PUBLICATION OF COLLEGE INFORMATION

Information that is already in the public domain is exempt from the 2018 Act. It is the College Policy to make as much information public as possible, and in particular the following information will be available to the public for inspection.

- Names of College managers.
- List of staff.

11. SUBJECT CONSENT

In many cases, the College can only process personal data with the consent of the individual. In some cases, express consent must be obtained. Agreement to the College processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes data on criminal convictions.

12. PROCESSING SENSITIVE DATA

Sometimes it is necessary to process data about a person such as health, criminal convictions, race, gender and family details. Because this data is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will be asked to give express consent for the College to do this. Offers of employment or course places may be withdrawn should an individual refuse to consent to this without good reason.

13. EXAMINATION MARKS

Students will be entitled to information about their marks for both coursework and examinations. The College may withhold certificates and accreditation and/or references in the event that the full course fees have not been paid, or all books and equipment belonging to the College have not been returned.

14. ACCEPTABLE USE OF INFORMATION TECHNOLOGY POLICY

14.1 Strategic Approaches

The College seeks to promote and facilitate the proper and extensive use of information technology in the interests of learning, teaching and research, including business and community engagement partnerships. Whilst academic freedom will be respected, this also requires responsible and legal use of the technologies and facilities made available to students, staff and friends of the College.

This Policy is intended to provide a framework for the use of Athena Global Education (AGE) IT resources. It applies to all computing, telecommunication, and networking facilities provided at the College. It should be interpreted such that it has the widest application, in particular references to IT services should, where appropriate, be taken to include departmental or other system managers responsible for the provision of an IT service. This policy should be interpreted so as to encompass new and developing technologies and uses, which may not be explicitly referred to.

Users of commercial broadband services provided, or facilitated by, the College must abide by any specific policies associated with those services. Members of the College and all other users of the College's facilities are bound by the provisions of these policies in addition to this Acceptable Use of IT Policy.

It is the responsibility of all users of Athena Global Education (AGE) IT services to read and understand this policy and accept it.

14.2 Purpose of Use

College IT resources are provided primarily to facilitate a person's essential work as an employee or student or other role within the College. Facilities are also intended to help enhance the wider experience of students attending the College. No use of any IT service should interfere with another person's duties or studies or any other person's use of IT systems, nor bring the College into disrepute in any way.

College email addresses must be used for all official College business in order to facilitate auditability and institutional record keeping. All staff and students of the College must regularly read their College email.

15. AUTHORISATION

In order to use the computing facilities of the College, an individual must first be registered. Registration to use College services implies, and is conditional upon, acceptance of this Acceptable Use Policy.

The registration procedure grants authorisation to use the facilities of the College. Following registration, a username, password and email address will be allocated. Authorisation for other services may be requested by application to IT services or other providers of Information Technology based services.

Individually allocated usernames, passwords, certificates and email addresses are for the exclusive use of the individual to whom they are provided. The user is personally responsible and accountable for all activities carried out under their username. The password associated with a particular personal username must not be divulged to any other person, other than, in person, to known designated members of IT staff for the purposes of system support. No one may use, or attempt to use, IT resources allocated to another person, except when explicitly authorised by the provider of those resources.

All users must correctly identify themselves at all times. A user must not masquerade as another, withhold their identity or tamper with audit trails. A user must take all reasonable precautions to protect their resources. In particular, passwords used must adhere to current password policy and practice.

16. PRIVACY

It should be noted that systems staff have the ability to access all files, including electronic mail files, stored on any computer which they manage. It is also occasionally necessary to intercept

network traffic. In such circumstances appropriate staff will take all reasonable steps to ensure the privacy of service users. The College fully reserves the right to monitor email, telephone and any other electronically-mediated communications. Reasons for such monitoring may include the need to:

- ensure operational effectiveness of services;
- prevent a breach of the law, of this policy, or other College policy;
- investigate a suspected breach of the law, this policy, or other College policy;
- monitor standards;

Procedural guidelines will be published from time to time as a separate document. Such access will normally only be granted in the following circumstances:

- where a breach of the law or a serious breach of this or another College policy is suspected;
- when a documented and lawful request from a law enforcement agency such as the police or security services has been received;
- on request from the relevant Department or Section, where the managers or co-workers of the individual require access to email messages or files, which are records of a College activity, and the individual is unable e.g. through absence, to provide them.

The College sees student privacy as desirable but not as an absolute right; hence students should not expect to hold or pass on information which they would not wish to be seen by members of staff responsible for their academic work. In addition to when a breach of the law or of this policy is suspected, or when a documented and lawful request from a law enforcement agency, such as the police or security services, has been received, systems staff are also authorised to release the contents of a student's files, including electronic mail files, when required to by any member of staff who has a direct academic reason for requiring such access.

The use of computers in College-managed laboratories, and the software installed on them, is automatically logged and are password protected; staff and students are provided with their usernames and passwords.

After a student or member of staff leaves the College, files which are left behind on any computer system owned or managed on behalf of the College, including servers and electronic mail files,

will be considered to be the property of the College and are deleted once a computer system is restarted.

17. BEHAVIOUR (THE BASIS FOR EFFECTIVE LEARNING AND TEACHING)

No person shall jeopardize the integrity, performance or reliability of computer equipment, software, data and other stored information. The integrity of the College's computer systems is put at risk if users do not take adequate precautions against malicious software, such as computer viruses and associated malware. Reasonable care should also be taken to ensure that resource use does not result in a denial of service to others.

Conventional norms of behaviour apply to IT based media, just as they would apply to more traditional media. Within the College setting this should also be taken to mean that the tradition of academic freedom will always be respected. The College is committed to achieving an educational and working environment which provides equality of opportunity, and freedom from discrimination.

No user shall interfere or attempt to interfere in any way with information belonging to, or material prepared by, another user. Similarly, no user shall make unauthorised copies of information belonging to another user. The same conventions of privacy should apply to electronically held information as to that held on traditional media such as paper.

Users of services external to the College are expected to abide by any policies, rules and codes of conduct applying to such services. Any breach of such policies, rules and codes of conduct may be regarded as a breach of this Acceptable Use Policy and be dealt with accordingly. This includes social networking sites, blog and wiki services, bookmarking services and any other externally hosted services. The use of Athena Global Education (AGE) credentials to gain unauthorised access to the facilities of any other organisation is **strictly prohibited.**

Acceptable uses may include:

- personal email and recreational use of Internet services, as long as these are in keeping with the framework defined in this policy document and do not interfere with the duties, studies or the work of others;

- advertising via electronic notice boards, intended for this purpose, or via other College approved mechanisms.

However, such use must not be regarded as an absolute right and may be withdrawn if abused or if the user is subject to a disciplinary procedure.

18. DEFINITION OF UNACCEPTABLE USE

Unacceptable use of College computers and network resources may be summarised as:

- the retention or propagation of material that is offensive, obscene or indecent, except in the course of recognised research or teaching;
- intellectual property rights infringement, including copyright, trademark, patent, design and moral rights, including use internal to the College;
- causing annoyance, inconvenience or needless anxiety to others;
- defamation (genuine scholarly criticism is permitted);
- unsolicited advertising, often referred to as "spamming";
- sending emails that purport to come from an individual other than the person actually sending the message using e.g., a forged address;
- attempts to break into or damage computer systems, or data held thereon;
- actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software;
- attempts to access, or actions intended to facilitate access, to computers for which the individual is not authorised;
- using the College network for unauthenticated access;
- excessive IT use during working hours that significantly interferes with a staff member's work, or that of other staff or students;
- the retention or propagation of material or websites whose purpose is to promote terrorism, or which are directly linked to a proscribed terrorist organisation, except in the course of recognised research or teaching that is permitted under law.

These restrictions should be taken to mean, for example, that the following activities will normally be considered to be a breach of this policy:

- the downloading, uploading, distribution, or storage of music, video, film, or other material, for which an individual does not hold a valid license, or permission from the copyright holder;
- the use of peer-to-peer software and related applications to illegally download and/or share music, video, film, or other material, in contravention of copyright law;
- the publication on external websites of unauthorised recordings e.g. of lectures;
- the distribution or storage by any means of pirated software;
- connecting an unauthorised device to the College network i.e. one that has not been configured to comply with this policy and any other relevant regulations and guidelines relating to security and acceptable use;
- circumvention of network access control;
- monitoring or interception of network traffic without permission;
- probing for the security weaknesses of systems by methods such as port-scanning, without permission;
- associating any device to network access points, including wireless, for which you are not authorised;
- non-academic activities which generate heavy network traffic, especially those which interfere with others' legitimate use of IT services or which incur financial costs;
- excessive use of resources such as file-store, leading to a denial of service to others, especially when compounded by not responding to requests for action;
- opening an unsolicited email attachment, especially if not work or study-related;
- the deliberate viewing and/or printing of pornographic images;
- the passing on of electronic chain mail;
- posting of defamatory comments about staff or students on social networking sites;
- the creation of web-based content, portraying official College business without permission or responsibility;
- the use of College business mailing lists for non-academic purposes;
- the deliberate viewing or accessing of material or websites whose purpose is to promote terrorism or which are directly linked to a proscribed terrorist organisation.

Other uses may be unacceptable in certain circumstances. It should be noted that individuals may be held responsible for the retention of attachment material that they have received via email that they have read. Similarly, opening an attachment, received via unsolicited email, especially if clearly unrelated to work or study, which leads to widespread virus infection, may result in disciplinary action being taken.

19. DISCIPLINE

Staff or students who break this Acceptable Use Policy will find themselves subject to College disciplinary procedures. The IT Manager, as well as an individual's department, may take such disciplinary action. Individuals may also be subject to criminal proceedings. The College reserves its right to take legal action against individuals who cause it to be involved in legal proceedings as a result of their violation of licensing agreements and/or other contraventions of this policy.

20. DATA RETENTION POLICY

AGE will ensure that data pertaining to its employees, payrolls, students' queries, students' admissions, assignments submitted, assessment of students, institute documents and materials will be managed properly and protected, by following the guidelines given below.

• An outsourced IT company will be overall responsible for storing, retaining data and data protection. The company will develop CRM and LMS platforms for AGE to store and retain all data

• The Course Administrators will be responsible for data management at Institute level and protection of students' assignments, feedback, AGE documents and materials. The accountants will be responsible to ensure data protection of all employees, including the payroll.

21. STUDENTS DATA PROCESSING

• All students will be made aware of AGE data collection, storage and safeguarding policy. All personal confidential information of students will only be handled by earmarked responsible staff members and stored in AGE CRM and LMS. These will be accessible only to authorized staff members through IT security systems.

• Potential students' queries will be entered into the AGE CRM (Customer Relationship Management) system by Students' Counsellors and follow ups done by the respective Counsellors for the students they are dealing with.

• All potential students who are going to be registered with AGE and who supply their personal documentation, the same will be uploaded into CRM and access to such information only available to the respective stakeholders dealing with students' documentation.

• Students' assignments' submissions, including feedback will be done on AGE Learning Management System (LMS) by the students themselves and the faculties checking the assignments respectively. The Course Administrators will ensure that the data thereafter is accurate and up to date on LMS.

• All grievances and appeals by students will be kept confidential and dealt only by the Academic Committee or Student Affairs Committee. Students' confidential sensitive health data forwarded by them for extenuating circumstances, will be received by the respective Course Administrator. Such data will be kept as soft copies by the Course Administrators in a confidential folder in the computer.

• Regular day to day correspondence through emails, CRM, LMS will be preserved and archived for a period of 7 years at least.

• All assessments of students will be available on LMS for a period of 3 years and after archival, available on the server for a period of 7 years.

• It will be ensured that in case of any adverse effect on the CRM and LMS, where the data is likely to be hacked/ lost, back up of the data of these two platforms is always maintained in a separate server, so that any lost data can easily be retrieved. This will be the responsibility of the IT Company. Retention of Data when Course is Completed AGE will store and retain all assessment records, internal verification records, and candidate records of the achievements in the following manner:

• All candidates' information registered for each qualification will be stored in the AGE CRM (Customer Relationship Management) system as soft data.

• Thereafter the candidates will be registered on LMS for their academic achievement and results. All details of candidates' assessments, name of faculty/ assessor, date and outcome of result will be stored in LMS, including the back-up server, in case records get corrupted/ lost.

• All Internal Verification results and activities will be recorded separately as soft copies with the respective Course Administrators and information of the same will be available in students' respective assignments on LMS.

• All certificates claimed from Universities and awarding bodies will be maintained by Course Administrators as soft copies.

• All such above records will be retained for 7 years at least after the completion date of the course.

• All award data comprising Name, DOB, Modules Passed, Results, Programme and Module specifications data will be kept for 120 years.

22. RETENTION OF DATA

The College will keep some forms of data far longer than others. Because of storage problems, data about students cannot be kept indefinitely, but the length of storage will fully comply with awarding organisation and QAA guidelines. Specific data relating to student records will be kept as noted in the table below.

Nature and scope of data	**Responsibility of:**	**Period of storage**
Student Transcript and Diploma Supplement	Student Services	10 years
Records documenting awards and classifications	Student Services	10 years
Records documenting the handling of formal complaints made by individual students against the institution.	Student Services	5 years

Records documenting the handling of complaints by individual students where the formal complaints procedure is not initiated.	Student Services	5 years
Disciplinary cases where the outcome is permanent expulsion.	Student Services	5 years
Records documenting the handling of complaints by individual students where the formal complaints procedure is not initiated.	Student Services	5 years

23. RELEVANT ASPECTS OF THE (REVISED) UK QUALITY CODE

23.1 Expectations for Quality: Core Practices

- The provider designs and/or delivers high-quality courses.
- The provider has sufficient appropriately qualified and skilled staff to deliver a high-quality academic experience.
- The provider has sufficient and appropriate facilities, learning resources and student support services to deliver a high-quality academic experience.

23.2 Common Practices

- The provider reviews its core practices for quality regularly and uses the outcomes to drive improvement and enhancement.
- The provider's approach to managing quality takes account of external expertise.
- The provider engages students individually and collectively in the development, assurance and enhancement of the quality of their educational experience.