ATLP DATA PROTECTION POLICY

DOCUMENT CONTROL

Author/Contact:	Lucy Meade Tel: 0121 323 1190 Email: lmeade@arthurterry.bham.sch.uk	
Document Reference:	ATLP Data Protection Policy	
Version	01	
Status	Final	
Publication Date	October 2014	
Related Policies	• Child Protection • Acceptable Use of Internet and IT • Health and Safety Policy • Publication of FOI • Complaints	
Review Date	Bi – Annually: September 2015	
Approved/Ratified By	Trust Board	Date: 6/10/14

Data Protection Policy

1. RATIONALE

ATLP is committed to a policy of protecting the rights and privacy of individuals, including students, staff and others, in accordance with the DPA.

ATLP needs to process certain information about its staff, students and other individuals with whom it has a relationship for various purposes such as, but not limited to:

- the recruitment and payment of staff
- the administration of programmes of study
- the recording of a student's progress
- collecting fees
- complying with legal obligations to funding bodies and government

To comply with various legal obligations, including the obligations imposed on it by the Data Protection Act, 1998, the ATLP must ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

2. ASSOCIATED LEARNING PARTNERSHIP POLICIES

- Child Protection
- Acceptable Use Agreements
- Health and Safety Policy
- Complaints

3. COMPLIANCE

This policy applies to all governors/trustees, staff and students of the ATLP, Any breach of this policy, or of the Act itself will be considered an offence and the school's disciplinary procedures will be invoked.

As a matter of best practice, other agencies and individuals working with the ATLP and who have access to personal information, will be expected to read and comply with this policy as part of their induction. It is expected that departments or individuals who are responsible for dealing with external bodies will take the responsibility for ensuring that such bodies sign a contract which among other things will include an agreement to abide by this policy.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the DPA and other relevant legislation.

The Information Commissioners Office (ICO) gives further detailed guidance and the ATLP undertakes to adopt and comply with ICO guidance.

4. THE DATA PROTECTION ACT, 1998

This piece of legislation came into force on 1 March 2000. The DPA regulates the processing of personal data, and protects the rights and privacy of all living individuals (including children), for example by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a “subject access request‟ (sample held at Appendix A).

Personal data is information relating to an individual and may be in hard or soft copy (paper/ manual files; electronic records; photographs; CCTV images), and may include facts or opinions about a person.

The DPA also sets out specific rights for academy students in relation to educational records held within the state education system. These rights are set out in separate education regulations „The Education (Student Information) (England) Regulations 2000.‟ For more detailed information on these Regulations see the Data Protection Guide on the ICO website.

5. RESPONSIBILITIES UNDER THE DPA AND REGISTRATION

The ATLP will be the data controller under the terms of the legislation – this means it is ultimately responsible for controlling the use and processing of the personal data at each of the partnership schools.

The ATLP Head teachers are responsible for all day-to-day data protection matters, and will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling within the school.

The ATLP is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

The ATLP is responsible for ensuring that the notification is kept accurate. Details of the notification can be found on the ICO website.

Compliance with the legislation is the responsibility of all members of the ATLP who process personal information.

Individuals who provide personal data to the schools within the ATLP are responsible for ensuring that the information is accurate and up-to-date.

6. DEFINITIONS

Data Controller: Any individual or organisation who controls personal data, in this instance the ATLP schools.

Personal Data: Data which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if uncontrolled and published in the press, Internet or media. The ATLP assumes consent to publish images unless parents specifically ask that their child is excluded from images used on the school website, press , internet and media, parents ,may opt out when they join the school or any other time should the situation change.

Sensitive Personal Data: Personal data relating to an individual's race or ethnic origin, political opinions, religious beliefs, physical/mental health, trade union membership, sexual life and criminal activities.

Relevant Filing System: Also known as manual records i.e. a set of records which are organised by reference to the individual/their criteria and are structured in such a way as to make specific information readily accessible e.g. personnel records (kept in lockable cabinets) and student filing.

Data Subject: An individual who is the subject of the personal data, for example, employees and students.

Processing: Obtaining, recording or holding data or carrying out any operation on the data including organising, adapting, altering, retrieving, consulting, using, disclosing, disseminating, aligning, blocking, erasing or destroying the data.

Accessible Records: Any records which are kept by the Organisation as part of a statutory duty, e.g. student records, personal records.

Parent: Has the meaning given in the Education act 1996, and includes any person having parental responsibility or care of a child.

7. DATA PROTECTION PRINCIPLES

The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles. In order to comply with its obligations, ATLP undertakes to:

7.1 Process personal data fairly and lawfully

The ATLP will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller via the school's **websites and internal communication system**; the purposes of the processing; any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, based on the guidance

from the **Records Management Service** and any other information which may be relevant.

7.2 Process the data for the specific and lawful purpose for which it collected that data, and not further process the data in a manner incompatible with this purpose

ATLP schools will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.

7.3 Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed

ATLP schools will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this in mind. If any irrelevant data are given by individuals, they will be destroyed immediately.

7.4 Keep personal data accurate and, where necessary, up to date

ATLP Schools will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify their school within the ATLP if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of the schools to ensure that any notification regarding the change is noted and acted on.

7.5 Only keep personal data for as long as is necessary

ATLP schools will not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means that ATLP will undertake a regular review of the information held and implement a weeding process, usually at the end of the academic year, using the recommended guidance in the Records management toolkit.

ATLP schools will dispose of any personal data in a way that protects it.

7.6 Process personal data in accordance with the rights of the data subject under the legislation

Individuals have various rights under the legislation including:

- a right to be told the nature of the information the ATLP schools hold and any parties to whom this may be disclosed;
- a right to prevent processing likely to cause damage or distress;
- a right to prevent processing for purposes of direct marketing;

- a right to be informed about the mechanics of any automated decision making process that will significantly affect them;
- a right not to have significant decisions that will affect them taken solely by automated process;
- a right to sue for compensation if they suffer damage by any contravention of the legislation;
- a right to take action to rectify, block, erase, or destroy inaccurate data;
- a right to request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened;

ATLP schools will only process personal data in accordance with individuals‟ rights.

7.7 Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data

All members of staff are responsible for ensuring that any personal data which they hold is kept securely, technically and physically and not disclosed to any unauthorised third parties. Staff will be aware of their responsibilities on induction.

The ATLP schools will ensure that all personal data is accessible only to those who have a valid reason for using it.

ATLP will have in place appropriate security measures e.g.

- ensuring that hard copy personal data is kept in lockable filing cabinets/ cupboards with controlled access;
- keeping all personal data secure;
- password protecting personal data held electronically; ie e- portal, CMIS, Progresso.
- archiving personal data on tapes, backed up and secure in a fire proof area;
- placing any PCs or terminals, CCTV camera screens etc. that show personal data so that they are not be visible except to authorised staff.

In addition, ATLP will put in place appropriate measures for the deletion of personal data – manual records will be shredded or disposed of as “confidential waste‟, and appropriate contract terms will be put in place with any third parties undertaking this work. **Hard drives of redundant PCs will be wiped clean before disposal, or if that is not possible, destroyed physically**.

This policy also applies to staff and students who process personal data „off-site", e.g. when working at home, and in such circumstances additional care must be taken regarding the security of the data including staff laptops.

7.8 Ensure that no personal data is transferred to a country or a territory outside the European Economic Area unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

ATLP schools l will not transfer data to such territories without the explicit consent of the individual.

This also applies to publishing information on the Internet – because transfer of data can include placing data on a website that can be accessed from outside the EEA. On joining the schools the ATLP assumes consent based on information provided to parents before admission to school, unless otherwise informed.

8. CONSENT AS A BASIS FOR PROCESSING

Although it is not always necessary to gain consent from individuals before processing their data, it is often the best way to ensure that data is collected and processed in an open and transparent manner.

Consent is especially important when schools are processing any sensitive data, as defined by the legislation.

ATLP understands consent to mean that the individual has been fully informed of the intended processing through the privacy notice, whilst being of a sound mind and without having any undue influence exerted upon them. Consent will be sought where needed and considered on a case by case basis. Consent obtained on the basis of misleading information will not be a valid basis for processing and consent cannot be inferred from the non-response to a communication.

ATLP schools will ensure that any forms used to gather data on an individual will comply with the the schools **Privacy Notice** – formerly known as Fair Processing Notice which explains the use of that data, how the data may be disclosed, and also indicate whether or not the individual needs to consent to the processing.

ATLP will ensure that if the individual does not give their consent for the processing, and there is no other lawful basis on which to process the data, then steps will be taken to ensure that processing of that data does not take place.

8.1 Fair Processing

Under the "Fair Processing" requirements in the Data Protection Act, the ATLP Schools will inform staff and separately parents/carers of all students of the data they hold on the staff member or students, the purposes for which the data is held and the third parties (e.g. LA, DfE, QCA, etc.) to whom it may be passed. This fair processing

notice, now known as a Privacy Notice will be passed to staff when they join the ATLP and parents/carers through the admissions process. Parents/carers of young people who are new to the ATLP will be provided with the Privacy Notice.

9. SUBJECT ACCESS RIGHTS (SARS)

The Data Protection Acts extend to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Where a request for subject access is received from a student, the ATLP policy is that:

- Requests from students will be processed as any subject access request as outlined below and the copy will be given directly to the student, unless it is clear that the student does not understand the nature of the request for example in KS1 and KS2.
- Requests from students who do not appear to understand the nature of the request will be referred to their parents or carers.
- Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.

9.1 Processing Subject Access Requests

Requests for access must be made in writing.

Pupils, parents or staff may ask for a Data Subject Access form (see Appendix A). Provided that there is sufficient information to process the request, an entry will be made in the Subject Access log book, showing the date of receipt, the data subject‟s name, the name and address of requester (if different), the type of data required (e.g. Student Record, Personnel Record), and the planned date of supplying the information (normally not more than 40 days from the request date). Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be date on which sufficient information has been provided.

Note: In the case of any written request from a parent regarding their own child‟s record, access to the record will be provided within 15 school days in accordance with the current Education (Pupil Information) Regulations.

10. AUTHORISED DISCLOSURES

The ATLP schools, in general, only disclose data about individuals with their consent. However there are circumstances under which the **ATLP Data Protection officer** may need to be consulted on the disclosure of data without explicit consent for that occasion.

These circumstances are strictly limited to:

- Student data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations.
- Student data disclosed to authorised recipients in respect of their child‟s health, safety and welfare.
- Student data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school.
- Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters, (processing officers, for example in the LA, are contractually bound not to disclose personal data)
- Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the ATLP schools by teaching and non teaching staff, will only be made available where the person requesting the information is a professional legitimately working within the ATLP who need to know the information in order to do their work. The schools will not disclose anything on students‟ records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything where suggests that they are, or have been, either the subject of or at risk of child abuse.

10.1 Legal Disclosure

A “legal disclosure” is the release of personal information from the computer to someone who requires the information to do his or her job within or for the ATLP schools, provided that the purpose of that information has been registered.

10.2 Illegal Disclosure

An “illegal disclosure” is the release of information to someone who does not need it, or has no right to it, or one which falls outside the ATLP's registered purposes.

11. PUBLICATION OF INFORMATION

The schools within the ATLP publish various items which will include some personal data, e.g.

- Internal telephone directory
- Event information
- staff information

Staff records appertaining to individual staff will remain of a confidential nature

11.1 Email -

The contents of email may have to be disclosed in response to a request for information. Under the Regulation of Investigatory Powers Act 2000, Lawful Business Practice Regulations, any email sent to or from the school may be accessed by someone other than the recipient for system management and security purposes.

11.2 CCTV

There are some CCTV systems operating within ATLP for the purpose of protecting school members and property. ATLP schools will only process any personal data obtained by the CCTV system in a manner which ensures compliance with the legislation. CCTV is used extensively. By its very nature it is not possible to remove students from this but, we will only use footage for internal purposes or if it is officially requested by the police/ court of law.

For detailed guidance on CCTV see the ICO CoP on CCTV.

11.3 Images/Photographs

When recording images and audio, carried out by the news/ media, children/staff will only be named if there is a particular reason to do so (e.g. they have won a prize), and home addresses will never be given out.

Some examples of recordings and use are shown below though these are not exclusive. Please feel free to contact us should you have any concerns or require further information.

Internal

- Teaching & learning
- Displays
- Intranet
- Event Promotion

External

- Website
- Social Media – Such as Twitter
- Press/ Media Coverage
- Publications
- Exam boards
- Police/ Legal Request

12. DATA INTEGRITY

12.1 Data Accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the schools of a change of circumstances their computer record will be updated as soon as is practicable. A printout of their data record will be provided to data subjects every twelve months so they can check its accuracy, make any amendments and returned signed for updating the data.

12.2 Data Adequacy and Relevance

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the schools will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data. Staff data will be checked annually via Data Checking Sheets.

12.3 Length of Time

Data held about individuals will not be kept for longer than necessary for the purposes registered. Obsolete data will be properly erased and or disposed of.

13. IDENTIFICATION OF DATA

All ATLP staff, contractors working for it, and delivery partners will comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher.

All documents manual or digital that contain protected data will be labelled clearly, either as restricted or confidential (where it is sensitive personal information)

Users must be aware that when data is aggregated the labelling may need to be altered and a higher level labelling applied. In addition destruction/storage arrangements should be clearly labelled:

- Secure Encryption
- Securely delete or shred

Paper documents labelled confidential must be held in lockable storage.

The ATLP recognises that under Section 7 of the Data Protection Act, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject.

Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

14. DATA AND COMPUTER SECURITY

ATLP schools undertake to ensure security of personal data by the following general methods.

14.1 Physical Security

Appropriate building security measures are in place, such as alarms. Only authorised persons are allowed in Server and Hub rooms. Disks, tapes and printouts are locked away securely when not in use. Visitors to the schools are required to sign in and out, to wear identification badges whilst in the school are, where appropriate, accompanied.

14.2 Logical Security

- Security software is installed on all computers containing personal data**.**
- The schools IT Support team will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. The appropriate file permissions are set for persona and locations by the ICT Support team
- All users will be given secure user names and strong passwords. User names and passwords must never be shared. Passwords should be changed regularly. The systems are configured to enforce system wide password policy including enforcement of password history, password age, and minimum length and using upper and lower case alpha numeric characters.
- Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes. System administrators enforce auto locking of all machines via group policy.
- ***All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.****
- Personal data can only be stored on ATLP equipment (this includes computers and portable storage media).

- When personal data is stored on any portable computer system, USB stick or any other removable media schools must make every attempt to ensure the device is encrypted using IT Support encryption methods .
- the device must be password protected. System administrator must enforce that laptops and desktops, are on the “school ICT domain”.
- the device must have school approved virus and malware checking software; Systems administrators ensure that laptops and desktops/apple macs have Anti Virus installed which is regularly updating and scanning
- the data must be securely deleted from the device, in line with ATLP policy, i.e. once it has been transferred or its use is complete.
- The ATLP has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups. All backups are completed regularly, checked for validation and schools must have a facility for offsite storage.

14.3 Procedural Security

In order to be given authorised access to the computer, staff will have to undergo checks and will sign their contract to ensure they are aware of their Data Protection obligations and their knowledge updated as necessary.

Further information can be found in the Staff and Student Acceptable Use of Internet and IT Policy.

Overall security for system access to data is determined by the ICT Strategic Director and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent.

Any queries or concerns about security of data in the first instance should be referred to the DPA Officer.

Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

15. SECURE TRANSFER OF DATA AND ACCESS OUT OF ATLP SCHOOLS

The ATLP recognises that personal data may be accessed by users out of the schools, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or personal data from the ATLP authorised premises without permission and unless the media is encrypted

and password protected and is transported/sent securely in an encrypted format for storage in a secure location.

- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of the school .
- When data is required by an authorised user from outside the school premises (for example, by a teacher or student working from their home or a contractor) they must have secure remote access to the management information system (MIS) or learning platform.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved password techniques and encryption software**.**
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe.

16. DISPOSAL OF DATA

The schools will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of protected data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten and other media must be shredded, incinerated or otherwise disintegrated for data.

A Destruction Log will be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

17. TRAINING AND AWARENESS

All staff will receive data handling awareness/data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff;
- Staff meetings/briefings/Inset;
- Day to day support and guidance from the Responsible Person.

18. ENQUIRIES

Information about the ATLP‟s Data Protection Policy is available from the ATLP website, l information about the Data Protection Act can be obtained from the Information Commissioners Office http://www.ico.gov.uk/. A copy of this policy will be made available to all employees and covered in new staff Induction Training. It

will be reviewed annually, added to, or modified from time to time and may be supplemented in appropriate cases by further statements and procedures relating to the work of the particular groups of workers.

Appendix A - ACCESS TO PERSONAL DATA REQUEST (Subject Access Request – SARS)

DATA PROTECTION ACT 1998 (Section 7)

Enquirer's Surname: ……

Enquirer's Forenames: ……..

Enquirer's Address: ……

Enquirer's Postcode: ……

Enquirer's Tel No: ……

Are you the person who is the subject of the records you are enquiring about (i.e. the "Data Subject")?

YES / NO

If NO, Do you have parental responsibility for a child who is the "Data Subject" of the records you are enquiring about?

YES / NO

If YES, Name of child or children about whose personal data records you are enquiring:

……

Description of Concern / Area of Concern: ……

……

……

……

Description of Information or Topic(s) Requested (In your own words)

……

……

……

……

Additional Information

Please despatch Reply to: (if different from enquirer's details as stated on this form)

Name: ……

Address: ……

…….

DATA SUBJECT DECLARATION

I request that the School search its records based on the information supplied above under Section 7 (1) of the Data Protection Act 1998 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the School.

I agree that the reply period will commence when I have supplied sufficient information to enable the School to perform the search.

I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and Address above who I have authorised to receive such information).

Signature of "Data Subject" (or Subject's Parent)

_____

Name of "Data Subject" (or Subject's Parent) (PRINTED)

_____Date_____