	ATLAS Multi Academy Trust
General Data Protection Regulations (GDPR) Policy	
Trust sub-committee: Resources Committee	
Co-ordinator: ATLAS Executive Team	
Last Reviewed: Summer 2018	**Next Review: Summer 2020**
St Albans Girls' School : Beech Hyde Primary School and Nursery : Adeyfield School	
	
Signed by: **Margaret Chapman** ***Executive Head Teacher***	**Signed by:** **Rachael Kenningham** ***Chair of ATLAS Board of Directors***

1.	**INTRODUCTION**
1.1	This is an ATLAS Multi Academy Trust Policy, but relates to all the Schools within ATLAS. ATLAS Multi Academy Trust (the Trust) is the organisation which is in charge of the Trust and its School's personal information. This means that ATLAS is called the Data Controller. The Schools within ATLAS are referred to in this policy as 'the School' and the ATLAS Multi Academy Trust is referred to as 'the Trust. This GDPR Policy includes the Freedom of Information Policy. Privacy Notices are also available.
2.	**AIMS**
2.1	This policy aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.
2.2	This policy applies to all personal data, regardless of whether it is in paper or electronic format.
3.	**RESPONSIBILITIES**
3.1	This policy applies to all staff employed by the Trust (including Members, Directors, Trustees and Local Governing Body Governors) and to external organisations or individuals working on the Trust's behalf. Staff who do not comply with this policy may face disciplinary action.
3.2	***Board of Directors*** The Trust Board of Directors has overall responsibility for ensuring that the Trust and its Schools comply with all relevant data protection obligations.
3.3	***Data Protection Officer*** The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

	They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on Trust data protection issues. The DPO is also the first point of contact for individuals whose data the Trust processes, and for the ICO. The Trust's DPO is Matthew Hall. He can be contactable in writing at ATLAS Multi Academy Trust, St Albans Girls' School, Sandridgebury Lane, St Albans, Herts, AL3 6DB or by email on mkh@stags.herts.sch.uk.
3.4	***Head teachers*** The School Head Teachers / Executive Head/ Principal act as the representatives of the data controller on a day-to-day basis.
3.5	***All staff*** Staff are responsible for: • Collecting, storing and processing any personal data in accordance with this policy • Informing the Trust of any changes to their personal data, such as a change of address • Contacting the DPO in the following circumstances: o With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure o If they have any concerns that this policy is not being followed o If they are unsure whether or not they have a lawful basis to use personal data in a particular way o 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 o If there has been a data breach o Whenever they are engaging in a new activity that may affect the privacy rights of individuals o If they need help with any contracts or sharing personal data with third parties
3.6	***Members, Directors and LGB Governors*** Members, Directors and LGB Governors must inform the Trust of any changes to their personal data, such as a change of address.
4	**COLLECTING DATA**
4.1	The Trust collects and uses certain types of personal information about staff, students, parents and other individuals who come into contact with the Trust in order provide education and associated functions. The Trust may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding, and this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation and other related legislation. The GDPR applies to all computerised data and manual files if they come within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured in some way that it is searchable on the basis of specific criteria (for example using the individual's name to find their information), and if this is the case, it does not matter whether the information is located in a different physical location. This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation, and shall be reviewed every 2 years.

5	**PERSONAL DATA**
5.1	Personal data is information that identifies an individual, and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain. A sub-set of personal data is known as 'special category data'. This special category data is information that relates to: • race or ethnic origin • political opinions • religious or philosophical beliefs • trade union membership • physical or mental health • an individual's sex life or sexual orientation • genetic or biometric data for the purpose of uniquely identifying a natural person Special category data is given special protection, and additional safeguards apply if this information is to be collected and used. Information related to criminal convictions shall only be held and processed where there is legal authority to do so. The Trust does not intend to seek or hold special category data (previously known as sensitive personal data) about staff or students except where the Trust has been notified of the information, or it comes to the Trust's attention via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice. Staff or students are under no obligation to disclose to the Trust their race or ethnic origin, political or religious beliefs, whether or not they are a trade union member or details of their sexual life (save to the extent that details of marital status and / or parenthood are needed for other purposes, e.g. pension entitlements).
6	**THE DATA PROTECTION PRINCIPLES**
6.1	The six data protection principles as laid down in the GDPR are followed at all times: 1. personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met 2. personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes 3. personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed 4. personal data shall be accurate and, where necessary, kept up to date 5. personal data processed for any purpose(s) shall not be kept in a form which permits identification of individuals for longer than is necessary for that purpose / those purposes 6. personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures In addition to this, the Trust is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law (as explained in more detail below). The Trust is committed to complying with the six data protection principles. This means that the Trust will:

	• inform individuals about how and why we process their personal data through the Privacy Notices which we issue • be responsible for checking the quality and accuracy of the information • regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the Data Retention Policy • ensure that when information is authorised for disposal it is done appropriately • ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system, and follow the relevant Security Policy requirements at all times • share personal information with others only when it is necessary and legally appropriate to do so • set out clear procedures for responding to requests for access to personal information known as subject access requests • report any breaches of the GDPR in accordance with the guidelines.
7	**CONDITIONS FOR PROCESSING IN THE FIRST DATA PROTECTION PRINCIPLE**
7.1	The individual has given consent that is specific to the particular type of processing activity, and that consent is informed, unambiguous and freely given. The processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps with regards to entering into a contract with the individual, at their request. The processing is necessary for the performance of a legal obligation to which we are subject. The processing is necessary to protect the vital interests of the individual or another. The processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in us.
8	**USE OF PERSONAL DATA BY THE TRUST**
8.1	The Trust processes personal data on students, staff and other individuals such as visitors. In each case, the personal data must be processed in accordance with the data protection principles as outlined above.
8.2	**Students** The personal data held regarding students includes contact details, assessment / examination results, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information, and photographs. The data is used in order to support the education of the students, to monitor and report on their progress, to provide appropriate pastoral care, and to assess the progression of the Trust as a whole, together with any other uses normally associated with this provision in a school environment. The Trust may make use of limited personal data (such as contact details) relating to students, and their parents or guardians for fundraising, marketing or promotional purposes and to maintain relationships with students of the School, but only where consent has been provided for this. In particular, the Trust may: • transfer information to any association society or club set up for the purpose of maintaining contact with students or for fundraising, marketing or promotional purposes relating to the Trust but only where consent has been obtained first

	• make personal data, including special category data, available to staff for planning curricular or extra-curricular activities • keep the student's previous school informed of his / her academic progress and achievements e.g. sending a copy of the school reports for the student's first year at the School to their previous school; Use photographs of students in accordance with the Photograph Policy. Any wish to limit or object to any use of personal data should be notified to the Trust Business Manager in writing, which notice will be acknowledged by the Trust in writing. If, in the view of the Trust Business Manager, the objection cannot be maintained, the individual will be given written reasons why the Trust cannot comply with their request.
8.3	**Staff** The personal data held about staff will include contact details, employment history, information related to DBS checks, information relating to career progression, photographs, occupational pensions, next of kin, medical information, bank account details, national insurance number etc for payroll, car registration number. The data is used to comply with legal obligations placed on the Trust in relation to employment, and the education of children in a school environment. The Trust may pass information to other regulatory authorities where appropriate, and may use names and photographs of staff in publicity and promotional material. Personal data will also be used when giving references. Staff should note that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as "spent" once the period of the sanction has expired, the details of the incident may need to be kept for a longer period.
8.4	**Information relating to DBS checks** DBS checks are carried out on the basis of the Trust's legal obligations in relation to safer recruitment of Staff as stipulated in the Independent School Standards Regulations and the DBS information (which will include personal data relating to criminal convictions and offences) is further processed in the substantial public interest, with the objective of safeguarding children. Retention of the information is covered by the Records Retention Policy. Access to the DBS information is restricted to those staff who have genuine need to have access to it for their job roles. In addition to the provision of the GDPR and the Data Protection Act 2018, disclosure of this information is restricted by section 124 of the Police Act 1997 and disclosure to third parties will only be made if it is determined to be lawful. Any wish to limit or object to the uses to which personal data is to be used should be notified to the Trust Business Manager who will ensure that this is recorded, and adhered to if appropriate. If the Trust Business Manager is of the view that it is not appropriate to limit the use of personal data in the way specified, the individual will be given written reasons why the Trust cannot comply with their request.
8.5	**Other Individuals** The Trust may hold personal information in relation to other individuals who have contact with the School, such as volunteers and guests. Such information shall be held only in accordance with the data protection principles, and shall not be kept longer than necessary.
9	**SECURITY OF PERSONAL DATA**
9.1	The Trust will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of the

	GDPR Policy and their duties under it. The Trust will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons. For further details regarding security of IT systems, please refer to the ICT Policy.
10	**DISCLOSURE OF PERSONAL DATA TO THIRD PARTIES**
10.1	The following list includes the most usual reasons that the Trust will authorise disclosure of personal data to a third party: • to give a confidential reference relating to a current or former employee, volunteer or student • for the prevention or detection of crime • for the assessment of any tax or duty • where it is necessary to exercise a right or obligation conferred or imposed by law upon the Trust (other than an obligation imposed by contract) • for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings) • for the purpose of obtaining legal advice • for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress) • to publish the results of public examinations or other achievements of students of the Trust • to disclose details of a student's medical condition where it is in the student's interests to do so and there is a legal basis for doing so, for example for medical advice, insurance purposes or to organisers of school trips. The legal basis for this will vary in each case but will usually be based on explicit consent, the vital interests of the child or reason of substantial public interest (usually safeguarding the child or other individuals) • to provide information to another educational establishment to which a student is transferring • to provide information to the Examination Authority as part of the examination process; and • to provide information to the relevant Government Department concerned with national education. At the time of the writing of this Policy, the Government Department concerned with national education is the Department for Education (DfE). The Examination Authority may also pass information to the DfE.
10.2	The DfE uses information about students for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual students cannot be identified from them. On occasion the DfE may share the personal data with other Government Departments or agencies strictly for statistical or research purposes.
10.3	The Trust may receive requests from third parties (i.e. those other than the data subject, the School, and employees of the Trust) to disclose personal data it holds about students, their parents or guardians, staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allow disclosure applies; or where necessary for the legitimate interests of the individual concerned or the Trust. All requests for the disclosure of personal data must be sent to the Trust Business Manager, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.
11	**CONFIDENTIALITY OF STUDENT CONCERNS**
11.1	Where a student seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or guardian, the Trust will maintain confidentiality unless it has reasonable grounds to believe that the student does not fully understand the consequences of withholding their consent, or where the Trust believes

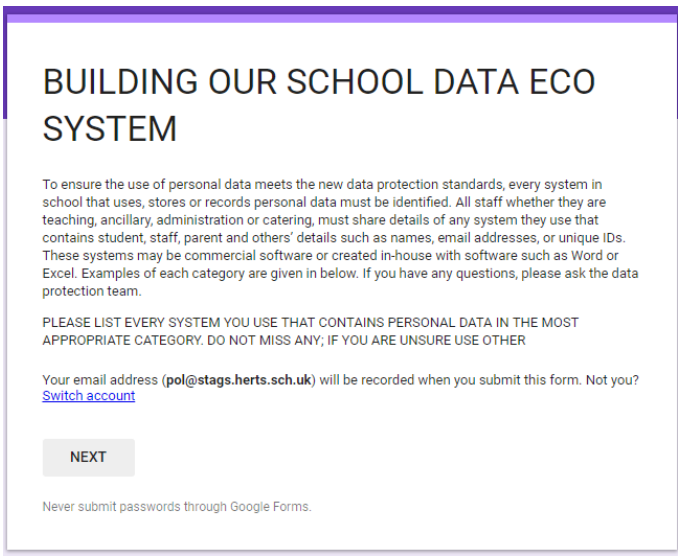
	disclosure will be in the best interests of the student or other students. Disclosure for a public safeguarding purpose will be lawful because it will be in the substantial public interest.
12	**SUBJECT ACCESS REQUESTS**
12.1	Anybody who makes a request to see any personal information held about them by the Trust is making a subject access request. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure, provided that they constitute a "filing system". A subject access request must be made in writing to the Trust. The Trust should send all requests to the Trust Business Manager within 3 working days of receipt. The Trust Business Manager must deal with the request in full without delay and at the latest within one month of receipt to the Trust Business Manager. The Trust may ask for any further information reasonably required to locate the information.
12.2	Where a child or young person does not have sufficient understanding to make his or her own request (usually those under the age of 12, or over 12 but with a special educational need which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. The Trust Business Manager must, however, be satisfied that: • the child or young person lacks sufficient understanding; and • the request made on behalf of the child or young person is in their interests
12.3	Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances the Trust must have written evidence that the individual has authorised the person to make the application and the Trust Business Manager must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.
12.4	Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).
12.5	An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected. All files must be reviewed by the Trust Business Manager before any disclosure takes place. Access will not be granted before this review has taken place. Where all the data in a document cannot be disclosed a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.
13	**EXEMPTIONS TO ACCESS BY DATA SUBJECTS**
13.1	Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived. There are other exemptions from the right of subject access. If we intend to apply any of them to a request, then we will usually explain which exemption is being applied and why.
14	**OTHER RIGHTS OF INDIVIDUALS**
14.1	The Trust has an obligation to comply with the rights of individuals under the law, and takes these rights seriously. The following section sets out how the Trust will comply with the rights to:

	• object to processing • rectification • erasure; and • data portability
14.2	**Right to object to processing** An individual has the right to object to the processing of their personal data on the grounds of pursu public interest or legitimate interest, where they do not believe that those grounds are adequately established. Where such an objection is made, it must be sent to the Trust Business Manager within 2 working days of receipt, and the Trust Business Manager will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings. The Trust Business Manager shall be responsible for notifying the individual of the outcome of their assessment within ten of working days of receipt of the objection.
14.3	**Right to rectification** An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received by the Trust, it should be sent to the Trust Business Manager within 2 working days of receipt. Where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable and the individual notified. Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data, and communicated to the individual. The individual shall be given the option of a review under the Data Protection Complaints Procedure, or an appeal direct to the Information Commissioner. An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.
14.4	**Right to erasure** Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances: • where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed • where consent is withdrawn and there is no other legal basis for the processing • where an objection has been raised under the right to object, and found to be legitimate • where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met) • where there is a legal obligation on the Trust to delete The Trust Business Manager will make a decision regarding any application for erasure of personal data, and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other data controllers, and / or has been made public, reasonable attempts to inform those controllers of the request shall be made.
14.5	**Right to restrict processing** In the following circumstances, processing of an individual's personal data may be restricted: • where the accuracy of data has been contested, during the period when the Trust is attempting to verify the accuracy of the data • where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure

	• where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim • where there has been an objection to the processing of personal data, pending the outcome of any decision
14.6	**Right to portability** If an individual wants to send their personal data to another organisation they have a right to request that the Trust provides their information in a structured, commonly used, and machine readable format. As this right is limited to situations where the Trust is processing the information on the basis of consent or performance of a contract, the situations in which this right can be exercised will be quite limited. If a request for this is made to the Trust, it should be sent to the Trust Business Manager within 2 working days of receipt, and the Trust Business Manager will review and revert as necessary.
15	**BREACH OF ANY REQUIREMENT OF THE GDPR**
15.1	Any and all breaches of the GDPR, including a breach of any of the data protection principles shall be reported as soon as it is discovered, to the Trust Business Manager. Once notified, the Trust Business Manager shall assess: • the extent of the breach • the risks to the data subjects as a consequence of the breach • any security measures in place that will protect the information • any measures that can be taken immediately to mitigate the risk to the individuals
15.2	Unless the Trust Business Manager concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the Trust, unless a delay can be justified. The Information Commissioner shall be told: • details of the breach, including the volume of data at risk, and the number and categories of data subjects • the contact point for any enquiries (which shall usually be the Trust Business Manager)~~;~~ • the likely consequences of the breach • measures proposed or already taken to address the breach If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the Trust Business Manager shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals. Data subjects shall be told: • the nature of the breach • who to contact with any questions • measures taken to mitigate any risks The Trust Business Manager shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the board and a decision made about implementation of those recommendations.
16	**CONTACT**
16.1	If anyone has any concerns or questions in relation to this policy they should contact the Trust Business Manager.

APPENDIX ONE – STAGS DATA ECO SYSTEM AUDIT

Audit undertaken of all staff week at STAGS commencing 26th March 2018 – results have been recorded and software recorded has been added to the GDPRiS software for to manage 3rd party suppliers that process data and streamline SARs & data breach reporting.
The same audit has been undertaken at Beech Hyde.



BUILDING OUR SCHOOL DATA ECO SYSTEM

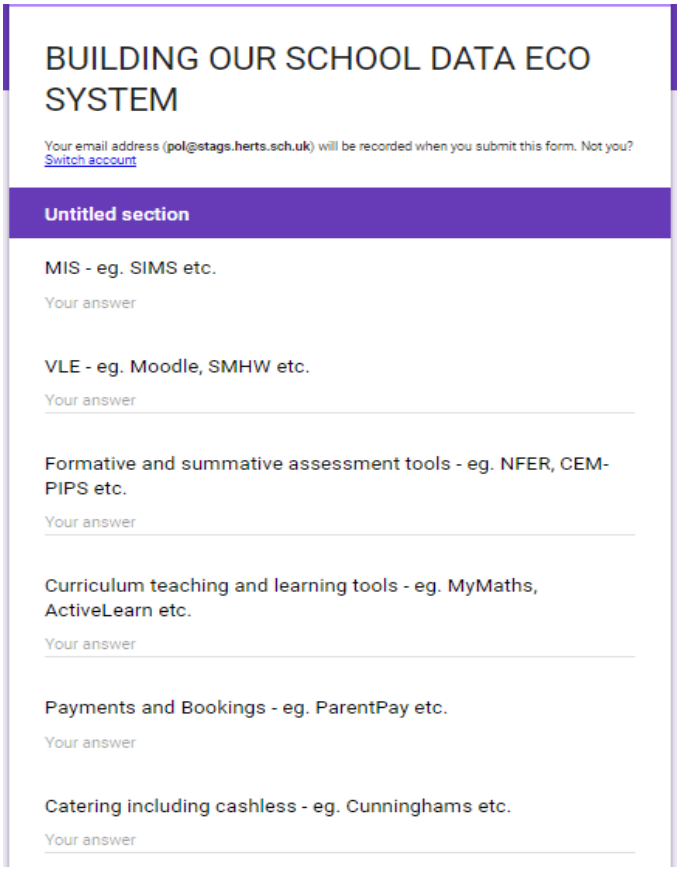
To ensure the use of personal data meets the new data protection standards, every system in school that uses, stores or records personal data must be identified. All staff whether they are teaching, ancillary, administration or catering, must share details of any system they use that contains student, staff, parent and others' details such as names, email addresses, or unique IDs. These systems may be commercial software or created in-house with software such as Word or Excel. Examples of each category are given in below. If you have any questions, please ask the data protection team.

PLEASE LIST EVERY SYSTEM YOU USE THAT CONTAINS PERSONAL DATA IN THE MOST APPROPRIATE CATEGORY. DO NOT MISS ANY; IF YOU ARE UNSURE USE OTHER

Your email address (**pol@stags.herts.sch.uk**) will be recorded when you submit this form. Not you? Switch account

NEXT

Never submit passwords through Google Forms.



BUILDING OUR SCHOOL DATA ECO SYSTEM

Your email address (**pol@stags.herts.sch.uk**) will be recorded when you submit this form. Not you? Switch account

Untitled section

MIS - eg. SIMS etc.

Your answer

VLE - eg. Moodle, SMHW etc.

Your answer

Formative and summative assessment tools - eg. NFER, CEM-PIPS etc.

Your answer

Curriculum teaching and learning tools - eg. MyMaths, ActiveLearn etc.

Your answer

Payments and Bookings - eg. ParentPay etc.

Your answer

Catering including cashless - eg. Cunninghams etc.

Your answer

IT Systems, Infrastructure and Services - eg. Active Directory etc.

Your answer

Leadership, Management, Office - eg. TargetTracker etc.

Your answer

Safeguarding tools - eg. SafetyNet etc.

Your answer

Communication tools - eg. SchoolComms etc.

Your answer

Uniform, equipment and photographs - eg. Magicard etc.

Your answer

Transport, travel and trips - eg. PlanMySchoolTrip etc.

Your answer

Identity and Data Collection Tools - eg. RMUnify

Your answer

External assessment and examination boards - eg. Edexcel, AQA

Your answer

References, careers and further education - eg. UCAS etc.

Your answer

Data transfer, aggregation,modelling, statutory returns and legal requirements - eg. GroupCall etc.

Your answer

Social and Health systems - eg. Capita One etc.

Your answer

Systems and tools outside the UK - eg. Apple Classroom

Your answer

Internal systems where no data is shared with a 3rd party - eg. Healthy Schools Survey, Microsoft Office etc.

Your answer

Other

Your answer

Send me a copy of my responses.

BACK SUBMIT

Never submit passwords through Google Forms.

FREEDOM OF INFORMATION POLICY

1	**INTRODUCTION**
1.1	The Trust is subject to the Freedom of Information Act 2000 (FOI) as a public authority, and as such, must comply with any requests for information in accordance with the principles laid out in the Act.
2	**WHAT IS A REQUEST UNDER FOI**
2.1	Any request for any information from the Trust is technically a request under the FOI, whether or not the individual making the request mentions the FOI. However, the Information Commissioner's Office has stated that routine requests for information (such as a parent requesting a copy of a policy) can be dealt with outside of the provisions of the Act. In all non-routine cases, if the request is simple and the information is to be released, then the individual who received the request can release the information, but must ensure that this is done within the timescale set out below. A copy of the request and response should then be sent to the Trust Business Manager. All other requests should be referred in the first instance to the Trust Business Manager, who may allocate another individual to deal with the request. This must be done promptly, and in any event within 3 working days of receiving the request. When considering a request under FOI, you must bear in mind that release under FOI is treated as release to the general public, and so once it has been released to an individual, anyone can then access it, and you cannot restrict access when releasing by marking the information "confidential" or "restricted".
3	**TIME LIMIT FOR COMPLIANCE**
3.1	The Trust must respond as soon as possible, and in any event within 20 working days of the date of receipt of the request. For example when calculating the 20 working day deadline, a 'working day' is a school day (one in which pupils are in attendance), subject to an absolute maximum of 60 working days (not school days) to respond.
4	**PROCEDURE FOR DEALING WITH A REQUEST**
4.1	When a request is received that cannot be dealt with by simply providing the information, it should be referred in the first instance to the Trust Business Manager, who may re-allocate to an individual with responsibility for the type of information requested. The first stage in responding is to determine whether or not the Trust "holds" the information requested. The Trust will hold the information if it exists in computer or paper format. Some requests will require the Trust to take information from different sources and manipulate it in some way. Where this would take minimal effort, the Trust is considered to "hold" that information, but if the required manipulation would take a significant amount of time, the requestor should be contacted to explain that the information is not held in the manner requested, and offered the opportunity to refine their request. For example, if a request required the Trust to add up totals in a spread sheet and release the total figures, this would be information "held" by the Trust. If the Trust would have to go through a number of spread sheets and identify individual figures and provide a total, this is likely not to be information "held" by the Trust, depending on the time involved in extracting the information.

4.2	The second stage is to decide whether the information can be released, or whether one of the exemptions set out in the Act applies to the information. Common exemptions that might apply include: • Section 40 (1) – the request is for the applicants personal data. This must be dealt with under the subject access regime in the DPA, detailed in paragraph 9 of the DPA policy above; • Section 40 (2) – compliance with the request would involve releasing third party personal data, and this would be in breach of the DPA principles as set out in the DPA policy above; • Section 41 – information that has been sent to the Trust (but not the Trust's own information) which is confidential; • Section 21 – information that is already publicly available, even if payment of a fee is required to access that information; • *Section 22 – information that the Trust intends to publish at a future date;* • *Section 43 – information that would prejudice the commercial interests of the Trust and / or a third party;* • *Section 38 – information that could prejudice the physical health, mental health or safety of an individual (this may apply particularly to safeguarding information);* • *Section 31 – information which may prejudice the effective detection and prevention of crime – such as the location of CCTV cameras;* • *Section 36 – information which, in the opinion of the Board of Directors of the Trust, would prejudice the effective conduct of the Trust. There is a special form for this on the ICO's website to assist with the obtaining of the chair's opinion.* The sections mentioned in italics are qualified exemptions. This means that even if the exemption applies to the information, you also have to carry out a public interest weighting exercise, balancing the public interest in the information being released, as against the public interest in withholding the information.
5	**CONTACT**
5.1	Any questions about this policy should be directed in the first instance to the Trust Business Manager.
6	**RESPONDING TO A REQUEST**
6.1	When responding to a request where the Trust has withheld some or all of the information, the Trust must explain why the information has been withheld, quoting the appropriate section number and explaining how the information requested fits within that exemption. If the public interest test has been applied, this also needs to be explained. The letter should end by explaining to the requestor how they can complain – either by reference to an internal review by [a governor], or by writing to the ICO.

APPENDIX ONE

Dear

Thank you for your request for XXXX information under the Freedom of Information (FOI) Act. I can acknowledge receipt of the request. As a Multi Academy Trust we are obliged to provide information under such requests. However before I can do this there are a couple of formalities I need to complete.

Firstly, in order for your request to be valid, we require a postal address from you - see "The Guide to Freedom of Information" (page 19) as published by the ICO. We will then write to you at this postal address and ask you to sign and return a copy of the letter, thus confirming that you have received the letter. We cannot treat your request as valid until this process is complete. Our practice is to reply formally to your response by post, although we will subsequently willingly provide information by email, where held in electronic form.

Secondly, I am sure you will be aware FOI requests can be time consuming on the part of the organisation dealing with the request, hence we have to make an assessment as to whether the request is vexatious. I would be grateful if you could confirm that your real name is XXXX, the reason for the request and whether you are making this request for your own purposes or on behalf of another organisation. This information is only being requested to allow us to make this assessment.

Finally, although this probably does not apply in your case, I would add we are aware a number of suppliers are using FOI to try to gain advantage in tendering for contracts. You should be aware where such information is deemed to be commercially sensitive we may not be able to provide it.

We are of course happy to receive expressions of interest from suppliers and to discuss opportunities to work with them. We often find this is a more productive way of developing a working relationship than using a blunt edged FOI request, which often puts additional strain on staff responsible for the areas concerned. You should be aware that if it proves to be the case that a Freedom of Information request has been used to try to obtain sensitive information, the Trust's policy is that persons or organisations making the requests are placed on a list of contractors with whom the Trust will not do business.

Yours sincerely

Mr P O'Neill
Business Manager

ATLAS Multi Academy Trust

Equality Impact Analysis

When reviewing all Trust policies, the following Equality Impact Analysis (EIA) should be undertaken to ensure fairness of the new proposals/policy and to identify any action needed to redress any potential discrimination, positively promoting equal opportunities, improved access and participation for all.

Title of Policy:	GDPR
Date:	Summer 2018
EIA carried out by:	P O'Neill
EIA reviewed by:	Resources Committee

1. Identify the aims and objectives of the policy, what will be the proposed change and how will it be implemented	
• **Policy contains information about:** Overall aims and objectives? What is the proposed change? Who is intended to benefit from the proposal and in what way? Outcomes of the policy? How will it be put into practice and who is responsible for this?	GDPR changes is legislation Roles and responsibilities for each school within the Trust Effects all staff and students

2. **Assessment of Impact?** *To include impact of policy, any plans needed to mitigate any negative impact, equality issues to be addressed*		
Characteristic	Group	Effect/Impact
• Age	Yes	Inclusive policy to meet the legal requirements of ATLAS as a date controller.
• Disability	Yes	
• Gender reassignment	Yes	
• Marriage/civil partnership	Yes	
• Pregnancy/Maternity	Yes	
• Race	Yes	
• Religion or Belief	Yes	
• Sex	Yes	
• Sexual orientation	Yes	

3. Consultation	
• **New policy contains information about:** Policy audience, expected actions and outcomes	Training programme in place to keep staff updated

Consultation and communication process Accessibility for all Fair access to the consultation process Lessons learnt from previous consultation, if appropriate	All staff have received refresher training in 2018 Staff have been consulted on the effects of GDPR

4. Decision	
• Should the new proposal/policy be agreed and any impacts identified following consultations? • What reasonable adjustments are required?	Staff and student privacy notices have been updated and made available via the school website

5. Action Planning	
• Any actions identified to address inequality for different groups? • Any actions identified to promote equality and diversity? • Where are these actions recorded and who is responsible for them?	None

6. Monitoring and Review	
• When will the impact assessment be reviewed? • Who is responsible?	Annually Trust Business Manager

7. Publication of the results of the impact assessment	
• Results of EIA are published – where and when? • The results are kept as a public record of the EIA – where and when?	With the policy