ATTENBOROUGH LEARNING TRUST

Attenborough Learning Trust

Data Protection Policy

Version: v 0.2

Version History

Version	Date	Edited By	Status	Comments
0.1	05/04/2019	Jo Marshall	Published	Initial Document
0.2	30/06/2021	Jane Ridgewell	Final	Aprroved at the Trust Board.

ATTENBOROUGH LEARNING TRUST

Data Protection Policy

Attenborough Learning Trust and our academies are committed to working effectively to provide a secure environment to protect data that we hold and store. Whilst there is a statutory duty that is important, the fact that we store data about individuals means that we are responsible for your data, and we take that very seriously. This policy, and the Privacy Notices, sets out how we look after and use data.

Each school will be responsible for the day-to-day management of data that is held about pupils, staff, parents, carers, and other individuals in connection with that school. The trust central team are responsible for data held centrally about individuals. Where we use the phrase 'we' that refers to the trust and the individual schools.

What is the General Data Protection Regulation (UK GDPR)?

This is a European Directive that was brought into UK law with an updated Data Protection Act 2018 (DPA) in May 2018. It was brought into line with changes to the UK leaving the Eu on 31 December 2020. The UK GDPR and DPA 2018 exist to look after individuals' data. It is a series of safeguards for every individual. Information about individuals needs to be treated with respect and be secure. The UK GDPR exists to protect individual rights in an increasingly digital world.

Who does it apply to?

Everyone, including schools. As 'Public Bodies' schools and trusts have more obligations than some small businesses. It is mandatory to comply with the UK GDPR and proposed provisions in the Data Protection Act 2018. We want to make sure information about pupils, parents, staff and volunteers is kept secure and within the law.

What is Data?

Any information that relates to a living person that identifies them. This can be by name, address, or phone number for example. It also relates to details about that person, which can include opinions. Some data is considered to be more sensitive, and therefore more important to protect. This is information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation, genetic data, and biometric data where processed to uniquely identify a person.

Schools often collect sensitive data for DfE and LA requirements and of course pupil data may contain information about safeguarding, SEN or health needs. Information about other family members may also be on the school file. Privacy Notices that explain how data about specific groups or activities is used and stored are also available. These can be obtained from each school and links on the website to UK GDPR compliance.

What are the key principles of the UK GDPR?

Lawfulness, transparency, and fairness

Schools must have a legitimate reason to hold the data, we explain this in the Data Privacy Notices. We often ask for consent to use data about a pupil for a particular purpose. If you wish to withdraw consent, we have a form to complete to allow us to process your request. There are sometimes when you cannot withdraw consent as explained in 'Data Subjects' Rights'.

Collect data for a specific purpose and use it for that purpose

Data cannot be used for a purpose that it was not originally collected for, or where notice has not been given about how data may be used after collection.

Limited collection

Data Controllers should only collect the minimum amount of data needed for a particular task or reason. If there is a breach or a hack only limited information can be lost.

Accuracy
Data collected should be accurate, and steps should be taken to check and confirm accuracy. This is done when pupils join the school and is reviewed on an annual basis. If a Data Subject feels that the information held is inaccurate, should no longer be held by the Controller or should not be held by the Controller in any event, a dispute resolution process and complaint process can be accessed, using the suitable forms. Initially an approach should be made directly to the individual school.

Retention
A retention policy is in place that governs how long records are held for.

Security
We have processes in place to keep data safe. That might be paper files, electronic records, or other information. Please see NAME YOUR POLICY OR LOCATION - AGAIN THIS SHOULD ULTIMATELY BE TRUST WIDE. The policy may be acceptable use, information security, IT policy or similar.

Who is a 'data subject'?
An individual whose details we keep on file. Some details are more sensitive than others. The UK GDPR sets out collection of details such as health conditions and ethnicity which are more sensitive than names and phone numbers.

Data subjects' rights
Individuals have a right: -

- To be informed.
- Of access to data stored about them or their children.
- To rectification if there is an error on the data stored.
- To erasure if there is no longer a need for school to keep the data.
- To restrict processing, i.e. To limit what is done with their data.
- To object to data being shared or collected.

There are other rights that relate to automated decision making and data portability that are not directly relevant in schools.

Data subjects' rights are also subject to child protection and safeguarding concerns and sharing information for the prevention and detection of crime. Schools also have legal and contractual obligations to share information with organisations such as the Department for Education, Social Care, the Local Authority and HMRC amongst others. In some cases, these obligations override individual rights.

These Data Subject's Rights are set out in more detail in the document 'My Rights – A Guide for Data Subjects'.

Subject Access Requests
You can ask for copies of information that we hold about you or a pupil (who you have parental responsibility for). This Subject Access Request process is set out separately. You need to fill out the form, and you may need to provide identification evidence for us to process the request.

We have to provide the information within a month, but this can be extended if the request is complicated, or the data cannot be accessed. When we receive a request, we may ask you to be more specific about the information that you require.

This is to refine any queries to make sure you access what you need, rather than sometimes getting a lot of information that may not be relevant to your query. In some cases, we cannot share all information we hold on file if there are contractual, legal or regulatory reasons. We cannot release information provided by a third party without their consent, or in some cases you may be better to approach them directly, e.g. school nurses who are employed by the NHS. We will supply the information by paper or electronic form. If you wish to complain about the process, please see our Complaints Policy and later information in this DPA policy.

Who is a 'Data Controller'?
The academy trust is the Data Controller. They have ultimate responsibility for how the schools and trust central team manage data. They delegate this processing to individuals to act on their behalf, that is the trust central team and the relevant school staff in each setting. The data controller can also have contracts and agreements in place with outside agencies who are data processors.

Who is a 'Data Processor'?
This is a person or organisation that uses, collects, accesses or amends the data that the controller has collected or authorised to be collected. It can be a member of staff, a third-party company, possibly a governor, a contractor or temporary employee. It can also be another organisation such as the police or the Local Authority.

Data Controllers must make sure that Data Processors are as careful about the data as the controller themselves. The UK GDPR places additional obligations on organisations to make sure that Data Controllers require contractual agreements to ensure that this is the case.

Processing data
The Trust and the schools must have a reason to process the data about an individual. Our Privacy Notices set out how we use data. The UK GDPR has 6 conditions for lawful processing and any time we process data relating to an individual it is within one of those conditions. If there is a data breach, we have a separate policy and procedure to follow to take immediate action to remedy the situation as quickly as possible.

The legal basis and authority for collecting and processing data in school are: -

- Consent obtained from the data subject or their parent.
- Performance of a contract where the data subject is a party.
- Compliance with a legal obligation.
- To protect the vital interests of the data subject or other associated person.
- To carry out the processing that is in the public interest and/or official authority.
- It is necessary for the legitimate interests of the data controller or third party.
- In accordance with national law.

In addition, any special categories of personal data are processed on the grounds of

- Explicit consent from the data subject or about their child.
- Necessary to comply with employment rights or obligations.
- Protection of the vital interests of the data subject or associated person.
- Being necessary to comply with the legitimate activities of the school.
- Existing personal data that has been made public by the data subject and is no longer confidential.
- Bringing or defending legal claims.
- Safeguarding.
- National laws in terms of processing genetic, biometric or health data.

Processing data is recorded within the school systems.

Data Sharing
Data sharing is done within the limits set by the UK GDPR. Guidance from the Department for Education, health, the police, local authorities, and other specialist organisations may be used to determine whether data is shared. The basis for sharing or not sharing data is recorded in school.

Breaches & Non Compliance
If there is non compliance with the policy or processes, or there is a DPA breach as described within the UK GDPR and DPA 2018 then the guidance set out in the Breach & Non Compliance Procedure and Process needs to be followed. Protecting data and maintaining Data Subjects' rights is the purpose of this policy and associated procedures.

Data Protection Breach & Non-Compliance Procedure
All staff, governors and trustees must be aware of what to do in the event of a DPA / GDPR breach. The 'Data Breach Flowchart' outlines the process. The 'Data Breach Form' will be completed and updated as the process progresses. Most breaches, aside from cyber criminal attacks, occur as a result of human error. They are not malicious in origin and if quickly reported are often manageable.
Everyone needs to understand that if a breach occurs it must be swiftly reported.

What is a breach?
A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

Examples of breaches are: -

- Information being posted to an incorrect address which results in an unintended recipient reading that information.
- Loss of mobile or portable data device, unencrypted mobile phone, USB memory stick or similar.
- Sending an email with personal data to the wrong person.
- Dropping or leaving documents containing personal data in a public place.
- Personal data being left unattended at a printer enabling unauthorised persons to read that information.
- Not securing documents containing personal data (at home or work) when left unattended.
- Anything that enables an unauthorised individual access to school buildings or computer systems.
- Discussing personal data with someone not entitled to it, either by phone or in person. How can you be sure they are entitled to that information?
- Deliberately accessing, or attempting to access or use personal data beyond the requirements of an individual's job role e.g. for personal, commercial or political use. This action may constitute a criminal offence under the Computer Misuse Act as well as the Data Protection Act.
- Opening a malicious email attachment or clicking on a link from an external or unfamiliar source, which leads to school's equipment (and subsequently its records) being subjected to a virus or malicious attack, which results in unauthorised access to, loss, destruction, or damage to personal data.

What to do?
Being open about the possible breach and explaining what has been lost or potentially accessed is an important element of working with the ICO and to mitigate the impact. Covering up a breach is never acceptable and may be a criminal, civil or disciplinary matter.

Report the breach to the Data Controller, Data Protection Compliance Manager and DPO as soon as possible, this is essential.

What happens next?
The breach notification form will be completed, and the breach register updated. Advice will be sought from the DPO. Consideration is given about how to effectively manage the breach, who to inform and how to proceed.

If the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach notification to those people will be done in a coordinated manner with support from the DPO.

Actions and changes to procedures, additional training or other measures may be required to be implemented and reviewed. The breach report will be within 72 hours of becoming aware of the breach. It may not be possible to investigate the breach fully within the 72 hour timeframe. Information about further investigations will be shared with the ICO with support from the DPO.

Procedure – Breach notification data controller to data subject
For every breach, the school will consider notification to the data subject or subjects as part of the process. If the breach is likely to be high risk, they will be notified as soon as possible and kept informed of actions and outcomes. The breach and process will be described in clear and plain language. If the breach affects a high volume of data subjects and personal data records, the most effective form of notification will be used and discussed with the Data Controller with support from the Data Protection Compliance Manager and DPO. Advice will be taken from the ICO about how to manage communication with data subjects if appropriate. A post breach action plan will be put into place and reviewed.

Evidence Collection
It may be necessary to collect information about how an information security breach or unauthorised release of data occurred. This evidence gathering process may be used as an internal process (which can include disciplinary proceedings), it may be a source of information for the ICO, it could also be used within criminal or civil proceedings.

This process will be conducted by a suitable member of school staff, which may be the Data Management Compliance Officer or Data Protection Officer but will be determined depending on the nature of the breach. Guidance may be required from external legal providers and police may be involved to determine the best way to secure evidence. A record of what evidence has been gathered, stored and secured must be available as a separate log. Files and hardware must be securely stored, possibly in a designated offsite facility.

Consent
As a trust, where required, we will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory, and regulatory occasions when consent is not required.

Consent is defined by the UK GDPR as “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”. We may seek consent from young people also, and this will be dependent on the child and the reason for processing. This will largely be managed in individual schools.

Consent and Renewal

On the trust/school websites we have 'Privacy Notices' that explain how data is collected and used. It is important to read those notices as it explains how data is used in detail. Obtaining clear consent, where required, and ensuring that the consent remains in place is important for school. We also want to ensure the accuracy of that information.

For Pupils and Parents/Carers
On joining the school you will be asked to complete a form giving next of kin details, emergency contact and other essential information. We will also ask you to give consent to use the information for other in-school purposes, as set out on the data collection/consent form.

The contact and consent form is reviewed on an annual basis. It is important to inform school if details or your decision about consent changes. A form is available. This is the obligation of each individual to notify the school of changes.

Pupil Consent Procedure
Where processing relates to a child under 13 years old, school will obtain the consent from a person who has parental responsibility for the child as required. Pupils may be asked to give consent or to be consulted about how their data is obtained, shared and used in certain situations.

Withdrawal of Consent
Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent the school will consider each situation on the merits and within the principles of UK GDPR and also child welfare, protection and safeguarding principles. Please complete the appropriate form.

CCTV Policy
We use CCTV and store images for a period of time in line with the policy. CCTV may be used for: -

- Detection and prevention of crime.
- School staff disciplinary procedures.
- Pupil behaviour and exclusion management processes.
- To assist the school in complying with legal and regulatory obligations.

Data Protection Officer
We have a Data Protection Officer whose role is: -

- To inform and advise the controller or the processor and the employees who carry out processing of their obligations under the UK GDPR.
- To monitor compliance with the UK GDPR and DPA.
- To provide advice where requested about the data protection impact assessment and monitor its performance.
- To be the point of contact for Data Subjects if there are concerns about data protection.
- To cooperate with the supervisory authority and manage the breach procedure.
- To advise about training and CPD for the UK GDPR.

Our DPO is John Walker whose contact details are:
Address:
Office 7, The Courtyard
Gaulby Lane,
Stoughton
LE2 2FL
Email info@jawalker.co.uk

Physical Security
As a trust we are obliged to have appropriate security measures in place. In school, every secure area has individuals who are responsible for ensuring that the space is securely maintained and controlled if

unoccupied, i.e. locked. Offices and cupboards that contain personal data should be secured if the processor is not present.

The Headteacher is responsible for authorising access to secure areas along with the School Business Manager. All Staff, contractors and third parties who have control over lockable areas must take due care to prevent data breaches. All sites and locations need to have the suitable security and review measures in place.

Secure Disposal
When disposal of items is necessary a suitable process must be used. This is to secure the data, to provide a process that does not enable data to be shared in error, by malicious or criminal intent. These processes, when undertaken by a third party are subject to contractual conditions to ensure UK GDPR and DPA compliance.

Complaints & the Information Commissioner Office (ICO)
The school Complaint Policy deals with complaints about Data protection issues. There is a right to complain if you feel that data has been shared without consent or lawful authority.
You can complain if you have asked to us to erase, rectify, or not process data and we have not agreed to your request. We will always try to resolve issues on an informal basis, and then through our formal complaints procedure. Please complete the form, and we will contact you with more details about the timescale and process.

In the UK it is the ICO who has responsibility for safeguarding and enforcing the DPA obligations. Email: casework@ico.org.uk
Helpline: 0303 123 1113
Website: www.ico.org.uk

Review
A review of the effectiveness of UK GDPR compliance and processes will be conducted by the Data Protection Officer every 12/24 months.

Appendix 1: CONFIDENTIALITY POLICY & CONFIDENTIALITY AGREEMENTS

Aim
To ensure that confidentiality and Data Protection Compliance are a natural part of good practice. To provide all staff, governors and others in school clear, unambiguous guidance as to their legal and professional roles. To make certain that the procedures throughout the school can be easily understood by pupils, parents/carers and staff.

Rationale
Schools hold a lot of confidential information about children, staff and sometimes parents and carers. Whilst it is important that we continue to develop positive ways to use that information, we all recognise that it is our responsibility to use, hold and safeguard information received.

The school is mindful that it is placed in a position of trust by all stakeholders and there is a general expectation that a professional approach will be used in all matters of confidentiality. Our obligation to comply with the Data Protection Act 2018, the UK GDPR and other legislation and statutory guidance underpins our management of data.

Objectives:
- To provide consistent messages in school about handling information about children and adults once it has been received.
- To foster an ethos of trust within the school.
- To ensure that staff, governors, volunteers, students, parents, and pupils are aware of the school's confidentiality policy and procedures.
- To reassure pupils that their best interests will be maintained.
- To encourage pupils to talk to their parents and carers.
- To ensure that pupils and parents/carers know that school staff cannot offer unconditional confidentiality.
- To ensure that if there are child protection issues then the correct procedure is followed.
- To ensure that confidentiality is a whole school issue and that everyone understands their personal responsibilities.

Guidelines
- All information about individuals is private and should only be shared with those staff that have a need to know.
- All social services, medical and personal information about a child should be held in a safe and secure place which cannot be accessed by individuals other than school staff.
- The school continues to actively promote a positive ethos and respect for the Individual.
- The Safeguarding Policy will be applied and monitored by appropriate school personnel.
- All children and adults have a right to the same level of confidentiality irrespective of gender, race, religion, medical concerns, and special educational needs.

Day to Day Practice
Confidentiality is a whole school issue. Even when sensitive information appears to be widely known it should not be assumed by those immediately involved that it is appropriate to discuss or share this information further.

Health professionals have their own code of practice dealing with confidentiality. Staff should be aware of children with medical needs and the class information sheet should be accessible to staff who need that information but not on general view to other parents/carers and children. Information about

children will be shared with parents and carers but only about their child. **Parents should not have access to any other child's books, marks, and progress grades at any time especially at parents evening.**

All personal information about children including social services records should be regarded as confidential. It should be clearly understood by those who have access to it, and whether those concerned have access to all, or only some of the information.

Information regarding health reports such as speech therapy, medical reports, SEN reports, SEN minutes of meetings and social services minutes of meetings and reports will be circulated in envelopes / files and once read should be returned for secure filing.

In all other notes, briefing sheets etc. a child should not be able to be identified. Addresses and telephone numbers of parents and children will not be passed on except in exceptional circumstances or to a receiving school.

Staff should exercise prudence and consider the dignity of individuals during conversations on the school site, for example in the staff room, particularly if non -members of staff are present and in the presence of children.

Non-members of staff, for example, students and voluntary helpers, will be asked to follow the principles of the confidentiality policy and sign a confidentiality agreement.

Governors/Trustees
Governors/Trustees need to be mindful that from time-to-time issues are discussed or brought to their attention about staff and children. All such papers should be marked as confidential and should be copied onto different coloured paper. These confidential papers should be destroyed after use.

Governors/Trustees must observe complete confidentiality when asked to do so by the governing body, especially in relation to matters concerning individual staff, pupils, or parents. Governors/Trustees will sign a confidentiality agreement annually.

Although decisions reached at governors' meetings are normally made public through the minutes or otherwise, the discussions on which decisions are based should be regarded as confidential.

Governors/Trustees should exercise the highest degree of prudence when discussion of potentially contentious issues arises outside the governing body.

Monitoring and Evaluation
The policy will be reviewed as part of the schools monitoring cycle.

Conclusion
Our trust has a duty of care and responsibility towards pupils, parents/carers, and staff. It also needs to work with a range of outside agencies and share information on a professional basis. The care and safety of the individual is the key issue behind this document.

Policy agreed by the Trust board and shared via the Trust website.

ATTENBOROUGH LEARNING TRUST

XXX School

Governor - Confidentiality Agreement

First of all, thank you for volunteering to be a Governor of this school. Your help and support in this role is greatly appreciated. In this role you are supporting the life of this school. This role carries certain responsibilities on your part including the requirement to be confidential about school matters. By signing this agreement, you agree to uphold XXX School's Confidentiality Policy. This means you will not share pupil / staff information with anyone other than those who are directly involved.

Examples of confidential information are (but not limited to):

- Information about staff and pupils.
- Information about actions of the Governing Body that are not published In Governing Body minutes.
- Information accessed by 'privilege' e.g. notices on staff noticeboard.
- Information about future school plans / actions than have not been disclosed to parents.

I understand that I may have access to confidential information and that it is my responsibility to maintain the integrity of this information and to keep it private. I further understand that disclosure of confidential information may result in termination of my membership of the Governing Body.

If I breach confidentiality, I understand that I may be in breach of the Data Protection Act 2018 and could face external sanctions.

Name of Governor	
Signature of Governor	
Date	
School Representative	
Signature of School Representative	
Date	

ATTENBOROUGH LEARNING TRUST

XXX School

Voluntary Helper - Confidentiality Agreement

First of all, thank you for volunteering to be a helper at this school. Your help and support in this role is greatly appreciated. In this role you are supporting the life of this school. This role carries certain responsibilities on your part including the requirement to be confidential about school matters. By signing this agreement, you agree to uphold XXX School's Confidentiality Policy. This means you will not share pupil / staff information with anyone that breaches confidentiality.

Examples of confidential information are (but are not limited to):

- Information about staff, pupils, and events that occur in school.
  For example, a parent who knows you are a helper at the school may ask you how their child is getting on (e.g. academically / behaviour). To prevent and misunderstanding, it would be better to advise the parent to speak to the class teacher.
- Information accessed by 'privilege' e.g. notices on staff noticeboard /conversations
- If you see something in school that concerns you, please discuss the matter with the head teacher.

I understand that I may have access to confidential information and that it is my responsibility to maintain the integrity of this information and to keep it private. I further understand that disclosure of confidential information may result in me no longer being required to be a volunteer.

If I breach confidentiality, I understand that I may be in breach of the Data Protection Act 2018 and could face external sanctions.

Name of Helper	
Signature of Helper	
Date	
School Representative	
Signature of School Representative	
Date	

ATTENBOROUGH LEARNING TRUST

XXX School
Student/Work Experience - Confidentiality Agreement

Please read the school's Confidentiality Policy. This work placement / experience carries certain responsibilities on your part including the requirement to be confidential about school matters. By signing this agreement, you agree to uphold XXX School's Confidentiality Policy. This means you will not share pupil / staff information with anyone that breaches confidentiality.

Examples of confidential information are (but are not limited to):

- Information about staff, pupils, and events that occur in school.
- Information accessed by 'privilege' e.g. notices on staff noticeboard /conversations.
- If you see something in school that concerns you, please discuss the matter with the head teacher.
- You must never use information about individual children outside the school without parental permission (photographs/names).

I understand that I may have access to confidential information and that it is my responsibility to maintain the integrity of this information and to keep it private. I further understand that disclosure of confidential information may result in me no longer being able to complete my placement as a student and that this breach may be reported to those who arranged the placement or my course leader.

If I breach confidentiality, I understand that I may be in breach of the Data Protection Act 2018 and could face external sanctions.

Name of Student	
Signature of Governor	
Date	
School Representative	
Signature of School Representative	
Date	

ATTENBOROUGH LEARNING TRUST

Appendix 2: Consent Forms

PLEASE NOTE THIS IS NOT A DEFINITIVE LIST OF CONSENT. THIS IS ONLY APPLICABLE FOR GDPR ISSUES – some schools choose to have other types of consent for climbing frame use, snowball fights, PE, and activities. IT fair usage polices, IT security policies, medical and pastoral information, discipline, behaviour and similar school management policies and arrangements are not covered within this list. Home School Agreement or Pupil Agreements must be considered separately.

THESE ARE NOT CONSIDERED AS PART OF UK GDPR COMPLIANCE

Photographs, Video and Media

	Yes	No
May we use your child's photograph in printed publications that we produce for promotional purposes such as a prospectus or on project display boards?		
I give consent for my child's image to be used on the school website and school social media		
May we record your child's image on video or webcam?		
I give consent for my child and their details to appear in the media. (for example in the local press, radio or TV)		
Are you happy for your child to appear on Social Media sites used by the school/college e.g. Twitter and Facebook ?		
I give consent for my son or daughter to be included in any school or class Yearbook and other mementos on leaving the school (if applicable)		
Do you consent for your son or daughter's name to be released for publication such that they may be identified as an individual or as part of a small group? For example raising money for charity that is recognised in the local media.		
I give consent for my son or daughter to be photographed for school group photos, that may be bought by other families who have children in the photo.		
I give consent for a professional photographer to take photographs and release to my family for sale? The photographer would have possession of the photos on their equipment, not school equipment.		
Are there any reasons why your child cannot participate in events and performances that may be recorded or photographed and shared with the school community? If yes please contact school to explain your concerns.		

Medical

Schools must have the right policy for children with medical conditions in schools. Consent from the parent/carer is essential before referring to the School Health Nursing Service, unless the referral is a self-referral from a young person deemed competent. You may wish to include this request as part of the consent and data collection forms. This should not replace your existing collection arrangements or policies.

Doctors Practice	
Doctors Name	
Telephone Number	
Does your child suffer from any health problems, if so please give details. (Please indicate any special treatment)	
Permission to contact Doctor	Yes/No (Please delete if appropriate)

Do you give consent for us to contact other professionals who are involved with your child?	Yes/No (Please delete if appropriate)
Names and contact numbers of any professionals involved with your child, for example health visitors, speech therapists. If you provide these details we will contact them, letting you know of any approach we make.	
Please give details of any other problems/concerns of which the school should be aware to enable us to support your child. If you provide these details we will contact them, letting you know of any approach we make.	
Please give details of any special requirements/medical conditions of parents/carers regarding access to the building or accessing information	

School Trips & Off-Site Visits

Please review your policies in respect of school trips. Acceptance of the risks, insurance issues and all other issues are subject to individual policies. This clause needs to be inserted. 'When making arrangements for school trips it is necessary to share information about your child with the venue, accommodation and transport providers for legal and safeguarding reasons. If travelling overseas this will also include immigration control. Details about your child may be required by insurers.'

For Trips Outside the UK

'Whilst pupils are outside the UK school staff and those supervising, travelling or arranging travel or accommodation may communicate with parents and carers using the contact information provided. At times this may be using mobile communications, social media or other methods that may require data to be stored or travel outside of the approved EU locations. We believe that keeping parents and carers informed about the wellbeing of their children must be the priority. Data sharing in such cases will be limited to what is necessary.

	Y	N
I give consent for school to take photographs of my son/daughter whilst on school trips.		
I give consent to school/college to take video and media footage of my son/daughter whilst on school trips		

Careers & Workplace Placements

	Y	N
I give consent for school/college to share details of my son/daughter with potential workplace placement providers		
I give consent to school/college to share details of my son/daughter with careers advisers		

School Work & Celebrating Successes

	Y	N
I give consent for school to share details of my son/daughter's achievements within school by displays, certificates or other media that identifies them		
I give consent to school/college to share information about my son/daughter to recognise key events such as birthdays within the school community		
I give consent for school/college to share details of my son/daughter's sporting activities for fixtures and achievements in school and in publications		

Internet Use

As part of the school's IT provision, we offer students access to the internet and email facilities. Our internet service provides a high level of protection, and we audit student use. Students are required to give written agreement to be bound by the terms.

	Y	**N**
As the parent or carer, I give permission for my child to use electronic mail and the internet. I understand that students are held accountable for their own actions.		

Childcare Costs, FSM, and PP

https://www.childcarechoices.gov.uk/

Parents and carers must be informed that they can check themselves.

	Y	**N**
I give consent for school/nursery to use my details, including National Insurance number, to check eligibility for Child Care place funding, Free School Meals and/or Pupil Premium		
I consent to the school/nursery to retain this information on file to continue to monitor eligibility		

School News Updates

	Y	N
I wish to be kept informed about school news and events and receive the newsletter and similar notifications		
I consent to the school to use text messaging service on the mobile number I have provided.		
I consent to the school contacting me by text message for the purpose of school information and reminders. I will ensure that I keep the school informed of my up to date mobile number at all times, or if the number is no longer in my possession		

(PLEASE NOTE: WE CANNOT ACCEPT INCOMING TEXT MESSAGES.)

Biometrics

YOU MUST PROVIDE DETAILS OF THE SCHEME ALSO AS ADDITIONAL INFORMATION

	Y	N
I give consent to information from the finger scan of my child (named above) being taken and used as part of an automated biometric recognition system for access to cashless dining facilities, library and in school ICT services. I understand that I can withdraw this consent at any time in writing.		

ATTENBOROUGH LEARNING TRUST

Third Parties at School

	Y	**N**
I give consent to the school to share basic details with third party providers, such as before and after school clubs, music and sport providers who may be engaged directly by me.		

Appendix 3: Consent

As a trust we will seek consent from staff, volunteers, young people, parents, and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory, and regulatory occasions when consent is not required. We may process personal and sensitive data without consent if another provision applies.

Consent is defined by the UK GDPR as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". We may seek consent from young people also, and this will be dependent on the child and the reason for processing. Pupils over 13 can give or withdraw consent.

Consent and Renewal

On the school website we have 'Privacy Notices' that explain how data is collected and used. It is important to read those notices as it explains how data is used in detail. Obtaining clear consent and ensuring that the consent remains in place is important for school. We also want to ensure the accuracy of that information.

When a pupil joins us, part of the process is to seek consent. This information is retained on the pupil file. If there are any changes, please inform us. We review the contact and consent form on an annual basis There will be a reminder about the need to update us throughout the school year.

For Pupils and Parents/Carers

On arrival at school, you will be asked to complete a form giving next of kin details, emergency contact and other essential information. We will also ask you to give consent to use the information for other in school purposes, as set out on the data collection/consent form.

Pupil consent procedure

Where processing relates to a child under 13 years old, school will obtain the consent from a person who has parental responsibility for the child. Pupil's may be asked to give consent or to be consulted about how their data is obtained, shared and used in certain situations.

Withdrawal of Consent

Consent can be withdrawn, subject to contractual, statutory, or regulatory constraints.
Where more than one person has the ability to provide or withdraw consent the school will consider each situation on the merits and within the principles of UK GDPR and also child welfare, protection and safeguarding principles.

ATTENBOROUGH LEARNING TRUST

Appendix 4: Information Security Policy

Aims of the Policy

1. To set out examples of good practice for the governance of personal data and information in all its forms, balancing the need to process and manage data set against risk of data breach.
2. To maintain and improve the security of our systems and the quality of our data by improving the data capability and awareness of our staff, students, and other users of the trust's data or computing and networking facilities and ensuring they are supported by appropriate tools and processes.
3. To ensure that appropriate technical and organisational measures are in place to prevent unauthorised access, damage or interference to and/or with information, IT assets and network services.
4. Both as an organisation and for individuals who process our data to ensure that that it we are aware of, and comply with, the relevant legislation as described in this and the other information governance and IT Policies.
5. To describe the principles of Information Security to members of staff, pupils and other authorised persons and to explain how these will be implemented by the trust.
6. To develop and maintain a level of awareness of the need for information security to be an integral part of the conducting of trust business and ensuring that everyone understands their individual and collective responsibilities in this respect.
7. To Protect personal data and other information held on our systems.
8. The impact of this policy will be to improve security and data management standards.
9. The terms 'personal data' and 'information' are used interchangeably in this policy, as are 'information security' and 'cybersecurity'.

This policy does not specifically address issues of privacy or personal data protection, although good data management and security are essential for compliance with data protection laws. Concerning privacy and data protection, the Data Protection Policy, Privacy Notices take precedence. This policy will be regularly reviewed and updated to ensure it remains current.

Relevant Legislation

There are many laws and regulations governing how information is handled, including:

- Common law in relation to duties of confidentiality.
- Regulation of Investigatory Powers Act 2000
- Data Protection Act 2018.
- Human Rights Act 1998
- Protection of Children Act 1999.
- Freedom of Information Act 2000.
- Computer Misuse Act 1990.
- Copyright, Designs and Patents Act 1988.
- Health and Safety at Work Act 1974.
- Theft Act 1978.
- Indecent display (Control) Act 1981.
- Obscene Publications Act 1984.
- UK General Data Protection Regulations 2018 (UK GDPR).

Personal Data

For purposes of this Policy, "Personal Data" means information that can identify an individual and is set out in the Data protection policy. It is important to note that some data is more sensitive and must be treated with greater care an understanding about the basis to process this sensitive data that includes:

- Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs.

- Trade-union membership.
- Genetic data, biometric data processed solely to identify a human being.
- Health-related data.
- Data concerning a person's sex life or sexual orientation.

Implementation of this Policy

- Staff and authorised persons awareness will be managed by training and induction.
- Regular testing of our IT and physical data safeguards.
- Evaluating the ability of each of our third-party service providers to implement and maintain appropriate security measures for the personal data to which we have permitted them access; and requiring such third party service providers by contract to implement and maintain appropriate security measures.
- Reviewing the scope of the security measures at least annually, or whenever there is a material change in our practices that may implicate the security or integrity of records containing personal data.
- Conducting an annual training session for all relevant people who have access to Personal data on the elements of the policy and keeping a record of attendees.

Storage of Information

The amount of personal data collected, and the time period for retention, should be limited to that amount reasonably necessary to accomplish our legitimate purposes, or necessary for the organisation to comply with other legal requirements, regulatory obligations and relevant advice from the Department for Education.

Systems to store data, including material from emails, will be in place to comply with our Record of Processing Activities. These may be physical or electronic/digital records.

Examples that set out more detail about good information management and security will be shared with staff and authorised persons. (see Twenty Tips for Staff – Toolkit Section 10) and Schedule 1 to this policy.

Physical Records — Records containing personal data (as defined above) must be stored appropriately, and records containing sensitive data should be stored in locked facilities, secure storage areas or locked cupboards or offices.

Electronic Records — To the extent technically feasible, the following security protocols must be implemented. Secure user authentication protocols including:

- Control of user ids and other identifiers.
- A reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices.
- Control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect.
- Restricting access to active users and active user accounts only.
- Blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system.

Secure access control measures that:

- Restrict access to records and files containing personal data to those who need such information to perform their job duties; and
- Assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls.

Encryption of the following:

- All transmitted records and files containing personal data that will travel across public networks, and encryption of all data containing personal data to be transmitted wirelessly.
- All personal data stored on laptops or other portable devices.
- Reasonable monitoring of systems, for unauthorised use of or access to personal data.
- For files containing personal data on a system that is connected to the internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal data.
- Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions and is set to receive the most current security updates on a regular basis.

Access to Information

Access to records containing personal data shall be restricted to current employees or approved persons who are reasonably required to know such information in order to support the trust's objectives.

Records containing Personal data shall only be removed from the site with specific authorisation from a relevant member of SLT or as part of an employee's job description. Staff and approved persons who have access to personal data will logoff their computers when not in use for an extended period of time.

During short periods of inactivity, these staff and approved persons will either lock their computers at the operating system level or ensure that no unauthorised person can gain access - this is of particular importance for computers or devise in classrooms or teaching areas if the device or computer is left unattended at any point.

Visitors to the site where personal data is stored shall not be permitted to visit any area of the premises that contains personal data unless they are escorted by a trust employee. Employees are encouraged to report any suspicious or unauthorized use of Personal data.

Transmission of Information

To the extent technically feasible, all records and files containing personal data which are transmitted across public networks or wirelessly must be encrypted or secured. Staff and authorised persons are prohibited from keeping open files containing sensitive personal data on their desks or in their work or teaching areas when these are unattended by a member of staff or authorised person.

At the end of the school day, all files and other records containing personal data must be secured in a manner consistent with this policy.

Disposition/Destruction of Information

Paper and electronic records containing personal data must be disposed by a secure and approved method that is understood by all staff or authorised persons.

Any temporary or permanent staff who leave the trust must return all records containing personal data, in any form, which may at the time of such termination be in the former persons' possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.)

Training

A copy of this Policy will be distributed to each employee or authorised person, (as well as visitors and suppliers as appropriate), who will have access to personal data. All such persons shall, upon receipt of the Policy, acknowledge in writing that he/she has received, read and understood it.

When the Policy is first issued, there will be training of employees and temporary employees who have access to personal data on the detailed provisions of the policy. All employees shall be retrained regularly.

All attendees at such training sessions are required to certify their attendance at the training and their familiarity with the company's policy and procedures for the protection of personal data.

Breaches
Breaches of the policy will be investigated and may be met with disciplinary action up to and including termination of employment. The nature of the disciplinary measures will depend on a number of factors including the nature of the violation. Any suspected breach should be reported immediately and the 'Breach and Non-Compliance' procedure is to be followed.

Third Parties
The contents of this Policy will apply to third parties who are intended to receive and process personal data.

Exceptions
Any exceptions to this policy require prior written authorisation and approval from the CEO.

Schedule 1

Good Practice Guise

The Data Protection Act 2018 sets out 6 principles concerning personal data, requiring that it must:

- Be processed fairly and lawfully.
- Be processed for specified purposes.
- Be adequate, relevant, and not excessive.
- Be accurate and up to date.
- Not be kept for longer than necessary for the specified purpose.
- Be processed in accordance with the rights of data subjects.
- Be protected by appropriate practical and organisational security.
- Not be transported (including electronically) outside the European Economic Area without ensuring protection for the data is at least as good as in the EEA.
- Parents and staff must be made aware that the information they give us may be recorded, may be shared in order to provide appropriate education and care, and may be used to support audit and other work to monitor the quality of education and care provided.

To do this we are all responsible for personal data when it is in our control.

Keeping Records Secure
All records that include student / staff identifiable information will be stored appropriately which may include securely in locked filing cabinets, password protected electronic databases or another form of restricted access storage when not in use depending on the sensitivity of the information contained in the records.

Employees are expected to take appropriate measures to ensure the security of personal data at all times, including keeping records secure attending meetings or removing records from site to work on at home. Access to computer equipment should be restricted by closing windows and doors when the room / office is not in use. Computer screens should always be locked (Ctrl, Alt and Del) if being left switched on and unattended.

Access will be afforded on a "need to do" basis, and access of leavers removed promptly.
So far as is reasonably practicable only authorised persons will be admitted to rooms that contain servers or provide access to data.

Equipment and paper files must not be left on view in any public setting. Computer monitors should be positioned in such a way that information stored or being processed cannot be viewed by unauthorised persons or members of the public. Documents or files containing personal identifiable information should be saved onto a shared network, with appropriate security protection, and not onto the C: Drive.

All school-owned ICT equipment, including software, should be recorded and security marked.
Users must not make, distribute or use unlicensed software or data on site. Mobile devices (e.g. laptops, memory sticks, etc.) must be encrypted for all sensitive, personal or confidential data.

Passwords
Passwords must not be shared with other members of staff under any circumstances.
Passwords should not be written down and/or left on display or be easily accessible.
Passwords should be "complex", comprising a combination of letters and numbers (preferably upper and lower case) and should be changed frequently.
The "remember password" feature should never be used.

Staff are encouraged to password protect any personal files, in particular those that contain potentially embarrassing information about an individual or an organisation.

Transfer / Sharing of Personal Data and/or Confidential Information
The Data Protection Act 2018 should be considered at all times when recording, sharing, deleting or withholding information.
Sensitive information must not be shared unless the person is authorised to receive it.

Email and Electronic sharing
Any transfers of confidential information should be secure, and the method risk assessed.
For electronic information transfers encrypted software should be used.

When information is requested by telephone it is important to:

- Ask the caller to confirm their name, job title, department and organisation and verify this by returning their call via their organisation's switchboard.
- Confirm the reason for the request.
- Be satisfied that disclosure of the requested information is justified.
- Place a record on the student / staff file noting the name of the person disclosing the information, the date and time of the disclosure, the reason for the disclosure, who authorised it (if applicable) and the recipient's details.

When sending personal or sensitive information by post:

- Check the name, department and address of the intended recipient.
- Use a robust envelope, clearly marked "**PRIVATE & CONFIDENTIAL To be opened by the addressee only**";
- Information to a service or department within the Local Authority should be sent using the internal post system;
- If the public post system is to be used a return address must be recorded on the outside of the envelope, and recorded delivery should be used if the information is considered to be highly sensitive.

EMPLOYEE ACKNOWLEDGEMENT FORM

I have received, read, and understand the Information Security Policy. I understand that it is my responsibility to comply with it.

Printed name: _____
Signature:_____
Date:_____

A SECURITY BREACH is any incident or activity that causes, or may cause, a break down in the availability, confidentiality, or integrity of the physical or electronic information assets of trust.

Appendix 5: Information Sharing – Good Practice

Many school policies refer to data sharing between schools and individuals or partner organisations. Data must be shared in compliance with the Data Protection Act 2018 and UK GDPR. Other statutory obligations and official guidance need to be considered when dealing with data sharing.

The DfE's Guidance on Information Sharing for Practitioners 2018 has a summary of these obligations. Overarching all policies should be a framework for information sharing which is driven by the key principles set out by the Government.

1. Necessary and proportionate. Data should only be shared with any third party, internally or externally, on the basis that it is proportionate to the need and fulfils the objective of the legitimate request. Different levels of risk will require individuals to make decisions on a case-by-case basis. Enough information should be provided to fulfil the policy or obligation.
2. Relevant. Relevant information should be shared with those who need it. This should be limited, and principles of data minimisation should be applied. Depending on the individual request, will determine the amount of information that is required.
3. Adequate. Information supplied should be fit for purpose and should be the right quality for the recipient to understand and be able to act upon it, rely upon it or understand it. Too little information is as dangerous as too much.
4. Accurate. Staff should be mindful to provide information that is as accurate as possible. This may require checking on school systems prior to giving information out. Reminders should be sent to parents, carers, and staff about updating information over the course of the academic year.
5. Timely. Information may be required on an urgent basis. Taking account of potential risks of not sharing information may lead to greater risks for pupils, or indeed adults. Sharing information needs to be on a timely basis, and on occasion requesters may have to be informed that a response will not be immediate. Realistic timescales should be shared.
6. Secure. Individuals must follow their own organisation's security measures. Processes for sharing personal and sensitive data should be applied in every case. Guidance around delivering information should be on a scale, the more sensitive the information the more care must be taken in sharing it.
7. Recording. Decisions in respect of information sharing should be recorded. Clearly the more sensitive the information being shared the more detail about why it was shared, who was shared with, how it was shared and the basis for sharing need to be in place. Day-to-day conversations do not need to be shared, emails and other correspondence may provide a suitable record if they have enough detail. Information should not be stored for longer than necessary and should be subject to retention policies and timelines.

When sharing information, it is important to understand the legal basis under UK GDPR. In many instances in schools, there is a legal duty to process information. However, it may also be by consent or part of a contract or as part of a public task. Sharing safeguarding and information that prevents or protects individuals from significant harm or requires immediate medical treatment to save and protect are dealt with under the category of vital interests.

Information requests from the Police, Social Care or Court Service need to be approached in the same way and properly considered about what information can, or could not be shared.

Information should be shared in accordance with policies.

If there is any question about the nature of information to be shared, or reasons for sharing, or not sharing, advice should be taken from the UK GDPR lead in school and the Data Protection Officer.

Appendix 6: Information Sharing Principles

Information sharing occurs on a daily basis in schools. It may be information about pupils, staff, parents or others. Every member of school staff, and many volunteers, have access to a lot of information about different individuals. For all of us, we have to bear in mind the basis that we share and discuss information. UK GDPR and Data Protection is only part of the story. Safeguarding, contractual responsibilities, statutory responsibilities and daily expectations are all other factors why we share information. Schools have many policies that deal with all aspects of school life. Every member of a school staff needs to consider some key elements when they are sharing information.

The purpose of sharing

Sharing information can be as simple as the word of a parent in the playground, by email or by telephone. It may be something as simple as "yes Tom had a good day" or "Kirpal enjoyed the music lesson". It might be far more intricate and complicated. It could be information about a child's injury at school. A health issue. Concern about behaviour, bullying or SEN. All of these are examples of information sharing.

Who are we sharing with?

Who is the recipient of the information? Do they have a legitimate right to know the information? Is it a parent or someone with Parental Responsibility? Is it an external partner agency like the police or social care? Is it an extended family member? Or even a sibling? Thinking about who the recipient is, and what is their legal basis for requesting the information, needs to be at the forefront of all school staff's consideration.

What data is to be shared?

Some information is more sensitive and sharing health information or safeguarding information must be done with great care. However, even some basic information about pupils or staff needs to be thought through carefully. When you are asked to share information, you need to consider what is the least amount of information that can be shared to fulfil the objective. Data minimisation is a key pillar of the UK GDPR – keep it as brief as possible.

Data quality, accuracy, relevance and usability

What information is being given? Is it an opinion or is it fact? If it is reporting information that is not known directly by you, what is the source of it? Are you sure it is accurate? Are you providing information that was given to school for one reason, but the requester wants it for a different purpose? If so, is it right to share that information?

Data security

How is the information to be shared? Face-to-face, is it a safe place to have a confidential conversation? Are other people around? Should confidential information be sent by email? What about secure delivery, or password protection? If being shared with an outside agency, what protections are in place? If information is going out by hard copy post, what checks and balances are there to make sure that the right recipients get the right report? (This is a common source of a data breach).

If information is going by pupil post, are there any risks if the bag went missing on the way home?
Are there measures in school to ensure that information is checked on an annual basis and reminders are sent through the academic year for parents and carers to update contact information?

Record-keeping

It will be impossible to keep track of every piece of information that is shared in the school. A school would grind to a halt within half an hour! However, sensitive information or safeguarding or health data being shared should be recorded. This might be as simple as keeping a note on an email about what was sent and why.

Individual's rights

All staff members should be aware that there are Data Subject Access processes that individuals can use. Likewise, there is a complaints process that can be accessed and people should be directed to the relevant pages on the school website or in the policies.

Appendix 7: Data Protection and the UK GDPR – My Rights

In a school setting, personal data is stored and used for a variety of reasons. You may be a parent, carer, pupil, staff member, governor, visitor or anyone else who the school store data about. There are a number of categories of people, and many different types of data that is used in schools on a daily basis. Whilst Privacy Notices set out details about why data may be collected, stored and used, there are some overriding principles that apply to every person (the Data Subject) when a school stores data. As Data Subjects, sometimes our consent is necessary for a school to process data about us. That might relate to photographs in school, reports in local press or similar. Consent is dealt with in the separate parts of the policy and can be accessed on the website or through the school office. There are other occasions when data about us or our children may be used by the school to fulfil a legal obligation, a contract or some other lawful usage. We all have other rights.

1. The right to rectification. Where data held about us is inaccurate, we have a right to apply for it to be amended and put right. This has to be done within one month, or within three months if it was complex. To do this we have to contact the data compliance manager within school, or the data protection officer. We have a right to complain if this is not done.
2. The right of access. This is a subject access request and is dealt with in more detail as part of the data protection policy. In essence, we have a right to see information about us that is classed as "personal data". There is a separate process for us to make this request within school, and the school may ask us to clarify or be more specific about what kind of data we are asking for if there is a lot of it. Again, there is a one month timeframe for this that can be extended for three months in complex cases.
3. We have a right to erasure. This means that in certain circumstances we can ask for data about us to be permanently deleted. However, this can be limited if the data needs to be kept for some official or lawful purpose. The right to erasure sometimes occurs if we withdraw consent to a process.
4. We sometimes have the right to restrict processing. If we believe that data is inaccurate, and we have asked for it to be erased, we can ask the data processor and controller to stop any processing until the investigation into erasure or amendment has taken place.
5. There is also the right to data portability, this has little bearing in the school setting. Transfer of data for pupils is regulated by guidance from the Department for Education. Data about staff is part of HMRC contractual obligations. Data portability would usually apply to things like utility companies or bank accounts.
6. Individuals also have the right to object to personal data being used for marketing. Again, in the school setting this is likely to be very limited as the only marketing tends to be limited to school fetes, fairs and plays. Schools and academy trusts should not be sharing data with commercial third party entities to enable direct marketing of individuals. If this was the case, then an individual could object and ensure that the data was no longer used for that purpose.
7. As individuals we also have the right to ask that decisions are made about us on the basis of our data, rather than by an automated process. Again, any application of this in schools would be extremely limited. This tends to be regarding situations such as reference agency checks for loans and mortgages for example.

These rights are important and sit alongside the school or trust's legal obligations to manage our data properly. Please also see the Privacy Notices and Data Protection Policy. If you feel that any of the Rights set out here are not being managed properly, or if that information held of our files is inaccurate or should not be there or should be changed or amended, please do let us know.

There is a form to complete at the end of this document. By providing us with as much detail as you can about why you think we have got something wrong, or why we are holding information that we should not be keeping, it makes the process much simpler for you.

We will respond within 28 days of receiving the form, and we will give our reasons in writing for any decision we make.

When you get the decision you can accept it, and you need do nothing more. You can ask for a review by us and our Data Protection Officer, you can complain using our policy if you feel that we have not acted

properly or you can make a referral to the Information Commissioner – whose details are found at https://ico.org.uk/ or by phone 0303 123 1113

Appendix 8: Attenborough Learning Trust Records Management Policy

Management of records is a legal obligation (Section 46 of the Freedom of Information Act 2000). By ensuring that our records are well managed and controlled we can provide a better service to staff, pupils, parents/carers and others. The legal and regulatory obligations from many sources rely on effective record management. Information management is also a part of the IT strategy, Data Protection and UK GDPR compliance obligations. This policy provides a framework that covers records management in the trust and the academies. It covers:

- Scope
- Responsibilities
- Relationships with existing policies

1. Scope

1.1 This policy applies to all records created, received or maintained by staff of the trust, whether centrally or in individual schools, in the course of carrying out its functions.

1.1 Records exist in the trust schools and originate from a variety of sources. Trust staff will create some. Others are provided by parents/carers and pupils, others are shared with the trust and its schools by external professionals. The policy applies to all records and the management of the records in the trust and its schools. See Appendix 1 for examples of records in the trust schools.

1.2 Records may be hard copy, electronic, digital, images, audio recordings or any other source that can be viewed, heard or interrogated. They may relate to individuals, financial planning, contracts, commercial organisations, public authorities or charitable organisations. Some will include personal data about individuals.

1.3 How the trust and schools use, maintain and manage records will be dependent on the purpose, origin and source of the records. Other policies will govern this in many instances.

1.3 Some records will be retained for historical and archiving purposes.

2. Responsibilities

2.1 The trust has a corporate responsibility to maintain, use, store and delete its records to comply with regulatory requirements. The person with overall responsibility for this policy is the Chief Executive Officer and this will be delegated to individuals in each school.

2.2 Good record management practice will be the responsibility of all staff. Individual responsibility will be determined by job description and practice. A senior leader (head, principal or head of school) will also monitor compliance with this policy at least annually.

2.3 Individual staff and employees must ensure that records for which they are responsible are accurate and are maintained and disposed of in accordance with the trust's policies and records management guidelines.

3. Relationship with existing policies

This policy has been drawn up within the context of:

- Freedom of Information policy
- Data Protection policy
- Information Security policy
- IT security and use polices
- Records retention policy/guidelines
- and with other legislation or regulations (including audit, equal opportunities and
- ethics) affecting the trust and schools.

Signed……..

Dated……..

The trust schools keep a wide variety of records that may include (but are not limited to):

Students

- Personal information.
- Parent/carer contact information.
- School reports.
- Behaviour logs.
- Exam and testing outcomes – internal and external.
- Child protection information.
- Allegations of a child protection nature made against a member of staff (including unfounded allegations).
- Attendance – attendance registers, authorised absence correspondence.
- SEND – reviews, advice to parents/carers, accessibility strategy.
- Pupil Premium / Sixth Form Bursary – evidence of eligibility.
- Free School Meals eligibility.
- Services and Pupil Premium eligibility.
- LAC status.
- Medical – Individual Health Plans, first aid records.
- Biometric records.

Management of the Trust and Schools

- Trust and Governing Board records - agendas, minutes, resolutions, reports.
- Trustee and Governors personal details.
- Declarations of Interests.
- CPD and training.
- Statutory Documents for Companies House.
- Accounts and Trust Report.
- School Development Plans and School Improvement plans.
- Leadership meetings, minutes, and actions.
- Admission details.
- School visitor logs.
- Health and Safety Records.
- Fire Risk Assessments.
- Risk Assessments.
- Social Media.
- Newsletters and external communication records.

Human Resources

- Job Descriptions.
- Application forms.
- Personnel files for all staff – including personal contact details.
- Appraisals.
- Performance reviews.
- Employment suitability checks.
- Contracts of employment.
- Records of Disciplinary and Grievances Process.
- Allegations and LADO referrals.
- Referrals to the TRA and/or DBS.
- Payroll and pensions – maternity/paternity pay, family leave records.

Financial Management

- Budgets and Funding details as required by the Funding Agreement, Academies Financial Handbook and Company Law.
- Risk Management and Insurance – employer's liability insurance certificate.
- Asset Management Records.
- Asset Register.
- All necessary financial records.
- Contracts.
- Contract Management and Procurement.
- School Payment and Meals Management.

Property Management

- Property Management.
- Condition Surveys.
- Hire agreements.
- Maintenance – log books, warranties and contractor information.
- Health and safety information.

Curriculum & Attainment

- Teaching and learning planning.
- Timetabling and resource planning.
- Prospectus and Website.
- Statistics and evidence of learning outcomes, targets.
- Pupil work records.
- Trip and visit record.

External Records

- Central Government and Local Authority.
- Local Authority – census returns, attendance returns.
- Central Government – returns made to DfE/ESFA.
- Ofsted.
- Referrals to third party agencies.
- Legal action involving the trust and schools.
- ICO action.
- Enquiries and investigations by external bodies.

ATTENBOROUGH LEARNING TRUST

Appendix 9 SAR request form

Data Subject (person who information is about)

Title	
Name	
Date of Birth	
Year group (if child or young person)	

Person making the request

Name	
Date of Birth	
Address	
Email Address	
Contact phone no	
Identification Evidence Provided (if required) Passport Driving licence Or two forms of Utility bill within last 3 months Bank statement of last three months Council Tax bill Rent book	

Status of person making request

Parent or person with Parental Responsibility	
Are you acting on their written authority (please provide a copy of the consent)	
If not the parent or with PR, what is your role?	

Details of Data Requested

Declaration

I, ……., hereby request that the Attenborough Learning Trust provide the data requested about me.

Signature:…….. Dated: …….

I, ……., hereby request that Attenborough Learning Trust provide the data requested about ……(insert child's name) on the basis of the authority that I have provided.

Signature:…….. Dated: …….

Appendix 10: Subject Access Request – Requester Overview

As an organisation we collect and process data about individuals. We explain what information we collect, and why, in our Privacy Notices.

- Any individual, person with parental responsibility, or young person with sufficient capacity to make a request, is entitled to ask what information is held. So that person is the 'Requester'. Copies of the information may also be made available on request.
- A form to complete is available.
- To ensure that requests are dealt with in an effective and timely manner we may seek to clarify the terms of a request.
- To collate and manage requests each school will have an individual allocated to co-ordinate all requests. **T**

That information is available on the school website and the Subject Access Request form.

What happens next?

There is a SAR request form on the website. We encourage everyone to use this form as it enables us to make sure you are being provided with the actual information that you require. Please complete the form, and provide the necessary information, and send it back to the school. Evidence of the requester's identity may be required. Discretion about employees and persons known to the school may be applicable but if ID evidence is not required an explanation must be provided by school staff and signed and dated accordingly. We may need to contact you to clarify details about what you have requested. We may need to contact other people and 3rd parties, who have provided information that is on our files.

Providing the Information

We need to review the information to see what can be shared, or if any item needs another person's consent. It may be that some information is subject to an exemption and cannot be shared. Exemptions to a SAR exist and may include:

- Education, Health, Social Work records
- Examination marks and scripts
- Safeguarding records
- Special educational needs
- Parental records and reports
- Legal advice and proceedings
- Adoption and Court records and/or reports
- Regulatory activity and official requests e.g. DfE statistical information
- National security, Crime and taxation
- Journalism, literature and art
- Research history, and statistics
- Confidential references

All data subjects have the right to know:

- What information is held?
- Who holds it?
- Why is it held?
- What is the retention period?
- That each data subject has rights. Consent can be withdrawn at any time (to some data).
- A right to request rectification, erasure or to limit or stop processing.
- A right to complain.

Much of this will be contained within the Privacy Notices and other information on our website.

Provision and Timeline

The information will be provided in an electronic format, usually within one calendar month of the request. However, in some circumstances if the request is complex or it is difficult to access the information, this may be extended by up to another 2 calendar months.

Information is usually provided in a secure electronic format.

Following delivery of the information the requester has the right to ask for a review or use the complaint process if they feel that information has not been provided.

Appendix 11: Trust Data Protection Management

Introduction - Overview

The Attenborough Learning Trust is committed to a policy of protecting the rights and privacy of individuals (including students, staff and others) in accordance with the Data Protection Act 2018. The Trust gathers and processes personal information about its staff, students, and other individuals to comply with obligations as a charitable company limited by guarantee that is responsible for academies. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

Any breach of the Data Protection Act 2018 or this Trust Data Protection Policy is considered to be an offence, and in that event relevant disciplinary procedures will apply. The contents of this policy are applicable to employees, trustees and governors, other agencies and providers working with the Trust, and who have access to personal information.

Attenborough Learning Trust is the Data Controller and is responsible for setting the overarching policy and standards for Data Protection. The trust see compliance with these obligations as the best method to ensure that personal information is dealt with lawfully and securely and in accordance with the UK GDPR and other related legislation.
It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically. It applies to all data held in schools as part of the multi-academy trust, though the responsibility for managing data rests with each school.

The Data Protection Policy and suitable Privacy Notices are on the trust website.
All schools within the trust process personal information about staff, pupils, parents and other individuals who come into contact with each academy as part of the usual day to day business of a school. The schools are 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 UK General Data Protection Regulation (UK GDPR) and other legislation.

This policy and procedures will be updated as necessary to reflect best practice, or amendments made to data protection legislation. Each academy within the trust will comply with the Trust policies, procedures and notices.

For Pupils and Parents/Carers

There is more detail in the 'My Rights' document and within the other policy and Privacy Notices on the website.

Pupil and Family Information Gathering

On joining an academy within the Trust you will be asked to complete a form giving next of kin details, emergency contact and other essential information. You will also be asked to give consent for the use of that information for other in-Trust purposes, as set out on the data collection/consent form. The contact and consent form will be reviewed on an annual basis. It is important to inform the Academy/Trust if details or your decision about consent changes. This is managed by each individual academy.

Subject Access Requests

As stated in our policy, every individual has a right of access, subject to some restrictions, to data that is held about them. If you wish to make a subject access request it is important that the request is

made directly to the school or academy that holds your data. There is more information about this process in the policy.

Concerns and Complaints
If you feel that something has gone wrong and you want to raise a complaint or concern it is important that you are able to do so. We encourage an informal discussion about the matter first. You can access details about how we manage such issues by reference to the complaints procedure. This also covers Data Protection and UK GDPR matters, though ultimately you have a right to refer to the Information Commissioners Office if you remain unsatisfied.

Data Protection Officer
Our Data Protection Officer is:

John Walker
Office 7
The Courtyard
Gaulby Lane
Sroughton
Leicestershire
LE2 2FL
info@jawalker.co.uk
www.jawalker.co.uk
03337 729763

Appendix 12: Consent Withdrawal Form - Adult

Please complete and deliver this form to the school office with your signature. Please note that as a school we may have contractual, statutory and/or regulatory reasons why we will still process and hold details of a pupil, parent, staff member, volunteer or other person.

Where two parents share parental responsibility, or where PR is shared, and the pupil is capable of expressing a view and there is conflict between the individuals the process of withdrawing consent will be subject to an evaluation and discussion to enable a decision to be reached that is considered to be in the pupil's best interests.

Withdrawal of consent for an individual

I, …… , withdraw consent for ……. (School name) to process my personal data. I withdraw consent to process my personal data for the purpose of
…… , which was previously granted.

Signed:

Date:

Received by school staff member:

Dated:

Actions:

Appendix 13: Consent Withdrawal Form – on behalf of Pupil
Please complete and deliver this form to the school office with your signature.
Please note that as a school we may have contractual, statutory and/or regulatory reasons why we will still process and hold details of a pupil, parent, staff member, volunteer or other person.

Where two parents share parental responsibility, or where PR is shared and the pupil is capable of expressing a view and there is conflict between the individuals the process of withdrawing consent will be subject to an evaluation and discussion to enable a decision to be reached that is considered to be in the pupil's best interests.

We may need to seek identification evidence and have sight of any Court Order or Parental Responsibility Agreement in some cases to action this request. If this is the case a senior member of school staff will discuss this with you.

Withdrawal of consent on behalf of a pupil

I, …… , withdraw consent in respect of …….. (Pupil Name) for …… (School name) to process my personal data. I withdraw consent to process their personal data for the purpose of …… , which was previously granted.

I confirm that I am …….. (Parent/Carer) and that I have parental responsibility for the pupil.

Signed:

Date:

Received by school staff member:

Dated:

Actions: