ATTENBOROUGH LEARNING TRUST

Attenborough Learning Trust

Information Sharing & Good Practice

Version: v 0.1

Version History

Version	Date	Edited By	Status	Comments
0.1	05/07/2022	Dave Nimmo	Published	

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.

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.

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.