Data Protection and GDPR Policy (Incorporating guidelines relating to General Data Protection Regulations)

Introduction

APTCOO (A PLACE TO CALL OUR OWN) collects and uses personal information about staff, learners, families, and other individuals who come into contact with the school. This information is gathered to enable APTCOO to provide education, care, and support to the highest standards. In addition, there are legal requirements to collect and use information to ensure that the organisation complies with the law and to fulfil the terms of its contracts.

Once APTCOO acquires personal information about learners, families and staff, we must keep this data secure. Unauthorised access or loss of information can cause serious harm to people.

This is governed by the Data Protection Act 2018 (also known as DPA or the UK GDPR). It incorporates previously existing EU data protection laws and is the main data protection legislation for the UK.

The Information Commissioner's Office (ICO) can issue fines if they learn that appropriate safety precautions are not being taken, and the maximum fine a business may face for non-compliance is up to £17 million or 4% of their global turnover (whichever is higher).

Both manual and digital records need to be secure. Therefore, the level of security we implement reflects the potential harm that could result from the loss or misuse of the data.

Furthermore, procedures are in place to respond to any security breaches.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely in accordance with the DPA and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored, and destroyed, no matter whether it is held in paper files or electronically.

All staff involved with the collection, processing, disclosure, and disposal of personal data will be aware of their duties and responsibilities by following these guidelines. Regular training updates will be available to staff to inform them of changes to legislation and to serve as a reminder of the importance of following the DPA.

Scope

APTCOO's data protection policy will incorporate the following people:

- Staff
- Learners and other children/young people who attend APTCOO settings.
- Families
- Volunteers and Trustees
- Visitors and third-party contractors/organisations.
- Anyone else who has dealings with APTCOO requiring the exchange of communication and/or information.

Not all security measures need to be complicated: sometimes just a simple check-in and check-out system can help reduce risks.

Terminology

Data subject: The person whom the personal data is about. In practice, this policy will call them “individuals”.

Processing: Almost anything done with data is counted as processing, including collecting, recording, storing, using, analysing, combining, disposing of or deleting it.

Data controller: a person, company or other body that determines the purpose and means by which personal data is processed. APTCOO is a data controller.

Data processor: anyone who handles personal data on the instructions of a controller (this does not include an employee of said controller, e.g., APTCOO in our case). Examples include storing, collecting, or analysing data as part of a service provided to the controller.

Personal information: defined as data which relates to a living individual who can be identified (either directly or indirectly) from that information, or other data held.

Privacy notices: these are outlines of what personal data APTCOO will require from individuals, what we will do with it and why, and which third parties we will pass it on to.

Special category data: This is personal data that needs more protection because it involves sensitive topics. They include the following:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data (where used for identification purposes)
- health data
- data concerning a person’s sex life
- sexual orientation.

To be processed, special category data must meet one of the following conditions:

(a) Explicit consent from the person it involves
(b) Employment, social security, and social protection (if authorised by law)
(c) Vital interests
(d) Not-for-profit bodies
(e) Made public by the data subject
(f) Legal claims or judicial acts
(g) Reasons of substantial public interest (with a basis in law)
(h) Health or social care (with a basis in law)
(i) Public health (with a basis in law)
(j) Archiving, research, and statistics (with a basis in law)

Statement of Intent

APTCOO (A Place to Call Our Own) is required to keep and process certain information about staff, volunteers and service users in accordance with its legal obligations under the General Data Protection Regulation (GDPR). APTCOO may, from time to time, be required to share personal information about staff, volunteers, or service users with other organisations, mainly the commissioning LA's, schools and educational bodies, and support services.

Organisational methods for keeping data secure are imperative, and APTCOO believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how APTCOO complies with the following core principles and requirements of the GDPR, which came into effect on 25 May 2018. The government have confirmed that the UK's leaving the EU will not affect the GDPR.

Consent

The DPA sets a high standard for consent. Consent means offering people genuine choice and control over how their data is used.

When consent is obtained and used properly it helps to build trust between APTCOO, families and other service beneficiaries.

APTCOO obtains specific consent from both individuals and families to retain contact information within our records, both electronically and hard copy, for the duration of the time they access our services. These take the form of privacy notices which will outline the data we collect, for what purpose we use it, and the rights of the individual regarding said data.

Child Protection and Safeguarding

In cases where the sharing of information with relevant organisations is necessary to protect a child from being (or at risk of being) harmed, data protection issues **must not stand in the way of ensuring the child's safety.** The law is very clear that child protection and safeguarding must come first, and you do not have to seek consent if to do so would potentially put a child or vulnerable adult at risk of immediate harm.

Processing

The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one lawful basis must apply whenever personal data is processed at APTCOO:

Help with identifying a lawful basis for processing can be found in the Other Resources section of Annex A in this document.

Practical Procedures

Before taking photographs of young people, ensure that APTCOO has explicit, written parental consent to do so. This should be found in the appropriate file folder and have been determined at the start of the child's placement at school.

Only use work devices to take and store images and other data regarding children and young people. APTCOO allows the sharing of work images within the Teams platform so long as no children or young people can be identified within them. Unaltered data is uploaded onto the secure Evidence for Learning platform to provide proof of a child or young person's work and achievements.

Work-related documents and data must not be downloaded to personal devices wherever possible. When this is not possible, you must ensure that said files are deleted as soon as possible.

Where photos are taken on personal devices to capture specific moments, they must be uploaded to the secure Sharepoint or EfL platform. After this is done, they must be deleted from the personal device with at least one other staff member present as a witness.

Where possible, when working on desktops and laptops, work should be undertaken and stored within APTCOO's Office 365 system. Documents, particularly those of a sensitive nature, should not be downloaded onto any device unless it is unavoidable. If so, when you have completed said work, ensure it is uploaded securely onto the system and delete the copy on the desktop/laptop.

All passwords should be updated every six months to ensure continued security and minimise the risk of data being compromised.

When using work devices, ensure that the latest security updates and patches are applied as and when they are released.

It is everyone's responsibility not to click or otherwise engage with suspicious links as these may introduce viruses which compromise security and put data at risk.

Disposal and deletion of data

When clearing work devices for increased storage purposes, ensure that images from iPads, cameras are backed up to SharePoint or the Evidence for Learning platform.

Where possible, when working on desktops and laptops, work should be undertaken and stored within APTCOO's Office 365 system. Documents, particularly those of a sensitive nature, should not be downloaded onto any device unless it is unavoidable. If so, when you have completed said work, ensure it is uploaded securely onto the system and delete the copy on the desktop/laptop.

Complaints

Complaints about any aspect of APTCOO's data procedures and practices should be made initially to the Chief Executive Officer who will decide, in consultation with the Chairperson of the Board of Trustees, whether it is appropriate for the complaint to be dealt with in accordance with APTCOO's complaint policy and procedure.

Complaints which are not appropriate to be dealt with through the APTCOO's complaint procedure can be dealt with by the Information Commissioner's Office.

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 3 years. The policy review will be undertaken by the Chief Executive Officer or nominated representative.

Contacts

If you have any enquiries in relation to this policy, please contact the Data Protection Officer Mike.Holmes@aptcoo.org who will also act as the contact point for any subject access requests.

Further advice and information are available from the Information Commissioner's Office, www.ico.org.uk or telephone 0303 123 1113.

Appendix 1

SUBJECT ACCESS REQUESTS

Procedures for responding to subject access requests made under the Data Protection Act 2018

Rights of access to information
There are two distinct rights of access to information held by schools about learners.

1. Under the Data Protection Act 2018 an individual has the right to make a request to access the personal information held about them.

2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (Wales) Regulations 2004.

These procedures relate to subject access requests made under the Data Protection Act 1998.

How to undertake an SAR can be found at the ICO's website: Your right to get copies of your data

Actioning a subject access request
1. Requests for information must be made in writing, including email, and be addressed to the Chief Executive Officer. If the initial request does not clearly identify the information required, then further enquiries will be made. A written request must be responded to within 15 school days, not including school holidays.

APTCOO must allow those with parental authority to view the record free of charge.
If a parent makes a request for a copy of the record, this must also be provided within 15 school days.

In most cases APTCOO will not and cannot charge a fee for an SAR relating to educational data. However, we may choose to charge an administrative fee if the request is 'manifestly unfounded or excessive' or if an individual chooses to request further copies of their data following a request. This fee will only cover supply costs.

2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- passport
- driving license
- utility bills with the current address
- birth / marriage certificate
- P45/P60
- credit card or mortgage statement

This list is not exhaustive

3. Any individual has the right to access information held about them. However, with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request.

The Chief Executive Officer should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian sha

APTCOO is exempt from providing education data in response to a SAR to the extent that complying with the request would be likely to cause serious harm to the physical or mental health of any individual. This is known as the "serious harm test" for education data.

More information on use of educational data and Pupil records and data protection guidelines can be found through the above links.

OTHER RESOURCES

LAWFUL BASES FOR PROCESSING

The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever personal data is processed at APTCOO:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

These privacy principles are supported by a further principle – accountability. This means that we must not only do the right thing with data but must also show that all the correct measures are in place to demonstrate how compliance is achieved.

5. The Dos and Don'ts

- Do not ignore. This can lead to financial penalties, enforcement action, legal proceedings, and reputational damage.
- Do not delay. Dealing with an SAR is time consuming so engage the appropriate personnel and start locating the information as soon as you receive an SAR.

- Liaise with the individual if you need further information to verify their identity or to enable you to locate the requested information.

- Locate the personal data. Consider electronic systems and manual filing systems, back up data and any third-party data processors (e.g., payroll and benefit providers) who may also hold relevant personal data.

- Redact information relating to other individuals unless you have their consent, or it is reasonable in all the circumstances to provide that information.

- Consider whether an exemption applies where the data would be exempt from disclosure.

- Respond to the request within the timeframe, provide copies of the relevant data and explain if and why you are relying on any of the exemptions.

6. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information, consent should normally be obtained; the 15-day period must continue to be adhered to.

7. Any information which may cause serious harm to the physical or mental health or emotional condition of the child/young person, or another should not be disclosed, nor should information that would reveal that the child/young person is at risk of abuse, or information relating to court proceedings.

8. If there are concerns over the disclosure of information then additional advice should be sought.

9. Where redaction (information which has been blacked out or removed) has taken place then a full copy of the information provided should be retained to establish if a complaint is made what was redacted and why.

10. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

11. Information can be provided at APTCOO with a member of staff on hand to help and explain matters if requested or provided at face-to-face handover. The views of the applicant should be ascertained when considering the method of delivery. If postal systems are used mail must be either registered or recorded delivery.

Other resources

Data rights: https://ico.org.uk/your-data-matters/

Pupil records and data protection guidelines

Lawful basis for processing interactive tool: https://ico.org.uk/for-organisations/gdpr-resources/lawful-basis-interactive-guidance-tool/

Appendix 2

Policy/ procedure for: Data Protection and GDPR

RECORD OF CHANGES

DATE	AUTHOR	PROCEDURE	DETAILS OF CHANGE
August 2017	Michelle Godfrey	Amendment to information	Website address for ICO updated (Page 6)
August 2017	Michelle Godfrey	Amendment to information	Telephone number for ICO updated (Page 6)
May 2018	Michelle Godfrey	Additional information relating to GDPR	Additional guidance for GDPR principles and changes to SAR request timeframes
October 2022	Mike Holmes	Updated information re: Data Protection and GDPR	V2 Annual review