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

Version Number: • 4	
Applies To: • APTCOO Charity Services • APTCOO Independent Special School • APTCOO Short Breaks • APTCOO Out of School Activities	
Associated Documents: • Staff Code of Conduct • Information Security & Acceptable Use Policy • Online Safety Policy	
Related Regulations: • UK General Data Protection Regulation (UK GDPR) • The Data Protection Act 2018 (DPA 2018) • The Charity Commission for England and Wales	
Review Frequency: • Annually	
Date of Implementation: • Autumn 2024	
Review Date: • Autumn 2025	
Chief Executive Officer (CEO) **Date 5/12/24**	**Chair of Board of Trustees /Governing Board** **Date 5/12/24**

Aims

APTCOO (A Place To Call Our Own) aims to ensure that all personal data collected about staff, learners, families, volunteers, governors and all other individuals who come into contact with APTCOO is stored and processed in accordance with UK data protection law.

This information is gathered to enable APTCOO to provide education, care, and support to the highest standards. However, we recognise that this data is often sensitive and requires careful protection.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

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

Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018 (DPA 2018)

This policy incorporates and draws from guidance published by the Information Commissioner's Office (ICO), which is the chief regulatory body for data protection.

It also reflects the ICO's guidance for the use of surveillance cameras and personal information gathered from such usage.

In addition, this policy complies with the Education (Independent School Standards) Regulations 2014 which provides minimum standards on information provision for independent schools.

Purpose

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.

Definitions

TERM	DEFINITION
Personal data	Any data which relates to a living individual who can be identified (either directly or indirectly) from that information.
Special category data	Personal data which is more sensitive and therefore needs more protection. This includes information about the following: • racial or ethnic origin • political opinions • religious or philosophical beliefs • trade union membership • genetic data • biometric data (such as fingerprints, retina and iris patterns, and where used for identification purposes) • health data – physical or mental • Sex life or sexual orientation.
Processing	Anything done to personal data, such as collecting, recording, organizing, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing, or destruction. Processing can be either an automated or a manual process.
Data subject	The identified or identifiable individual whose personal data is held or processed. In practice, this policy will call them "individuals".
Data controller	A person or organization that determined the purposes and means of processing personal data. APTCOO is a data controller.
Data processor	A person or organisation, other than an employee of the data controller, who processes personal data on behalf of the controller.
Privacy notices	This is a legal statement/document that outlines some or all the ways in which APTCOO will gather personal data, the purposes for which it will be used, and any/all third parties it may be passed on to.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss,

	alteration, unauthorised disclosure of, or access to, personal data.

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)

The Data Controller

APTCOO processes personal data relating to parents/carers, learners, other young people & families, staff, governors, volunteers, visitors, and others, and is therefore a data controller.

APTCOO is registered with the ICO and pays the relevant annual fee, as legally required.

Roles and Responsibilities

This policy applies to **all** staff and members of the APTCOO workforce, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Board of Trustees/Governing Board

The Board has overall responsibility for ensuring that APTCOO complies with all relevant data protection obligations.

Data Protection Lead

The data protection lead is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the Board their advice and recommendations on Organisational data protection issues

The Data Protection Lead is also the first point of contact for individuals whose data APTCOO processes, and for the ICO.

Full details of the Data Protection Lead's responsibilities are set out in their job description.

Our Data Protection Lead is Karen Kilner and is contactable via Karen.kilner@aptcoo.org

CEO

The CEO acts as the representative of the data controller on a day-to-day basis (This is delegated to the Headteacher in the case of the Independent Special School).

All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with the policy
- Informing APTCOO of any changes to their personal data, such as a change of address.
- Contacting the Data Protection Lead in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data, or keeping personal data secure.
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to reply on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK.
    - If there has been a data breach.
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties.

Data protection principles

This policy sets out how APTCOO aims to comply with these principles.

The UK GDPR is based on data protection principles that APTCOO always complies with.

The principles state that personal data must be:

- Processed lawfully, fairly, and in a transparent manner.
- Collected for specified, explicit, and legitimate purposes.
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary for the purposes for which it is processed.

- Processed and saved in a way that ensures it is appropriately secure.

.

Collecting personal data

Lawfulness, fairness and transparency

We will only process personal data where we have at least 1 of the 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that APTCOO can **fulfil a contract** with the individual, or the individual has asked APTCOO to take specific steps before entering into a contract.
- The data needs to be processed so that APTCOO can **comply with a legal obligation**.
- The data needs to be processed to ensure the **vital interests** of the individual or another person (i.e., to protect someone's life)
- The data needs to be processed for the **legitimate interests** of APTCOO (where the processing is not for any tasks APTCOO performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden.
- The individual (or their parent/carer when appropriate in the case of a learner/young person) has freely given clear **consent**.

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a learner/young person) has given **explicit consent**.
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**.
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made **manifestly public** by the individual.
- The data needs to be processed for the establishment, exercise or defence of **legal claims**.
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation.
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other personal obliged to confidentiality under law.
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health or social work professional or by any other personal obliged to confidentiality under law.

- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a learner/young person) has given **consent**.
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made **manifestly public** by the individual.
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**.
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not **reasonably** expect or use personal data in ways which have unjustified adverse effects on them.

Limitation, minimisation, and accuracy

We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary to do their jobs.
We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with APTCOO's record retention schedule.

Sharing personal data

APTCOO will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a learner/young person or parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- Our supplies or contractors need data to enable us to provide services to our staff and learners. When doing this, we will:
    - Only appoint supplies or contractors that can provide sufficient guarantees that they comply with UK data protection law.
    - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share.
    - Only share data that the supplier or contractor needs to carry out their service.

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them respond to an emergency situation that affects any of our staff or young people.

If and when were transfer personal data internationally, we will do so in accordance with UK data protection law.

Subject access requests and other rights of individuals

Subject access requests (SAR)

Individuals have a right to make a subject access request (SAR) to gain access to personal information that APTCOO holds about them. This includes:

- Confirmation that their personal data is being processed.
- Access to a copy of the data.
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period.
- Where relevant, the existence of the right to request rectification, erasure or restriction or to object to such processing.
- The right to lodge a complaint with the ICO or another supervisory authority.
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.
- The safeguards provided if the data is being transferred internationally.

Subject access requests can be submitted in any form, but APTCOO may be able to respond to requests more quickly if they are made in writing and include:

- Name of the individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a SAR in any form, they must immediately forward it to the Data Protection Lead.

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a SAR with respect to their child, the child must either be unable to understand their rights and the implications of a SAR or have given their consent.

Children **below** the age of 12 are generally **not** regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of children at APTCOO may be granted **without** the express permission of the child.

Children aged 12 and above are generally regarded **to** be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of children at APTCOO may **not** be granted **without** the express permission of the child.

Neither of these are rules, and a child/young person's ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made.
- Will respond without delay and within **1 month** of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within **3 months** of receipt of the request, where a request is complex or numerous. We will inform the individual of this within **1 month** and explain why the extension is necessary.

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the child or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent, and it would be unreasonable to proceed without it.
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

If the request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

Other data protection rights of the individual

In addition to the right to make a subject access request, and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time.
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing that has been justified on the basis of public interest, official authority, or legitimate interests.
- Challenge decisions based solely on automated decision making or profiling (i.e., making decisions or evaluating certain things about an individual
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO.
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the Data Protection Lead. If staff receive such a request, they must immediately forward it to the Data Protection Lead.

Parental requests to see the educational record

As an Independent Special School we are not required to give parents, or those with parental responsibility, a legal right to free access to their child's educational record (which includes

most information about a pupil); however, in line with DfE guidance for mainstream schools and academies, APTCOO will respond to any request from a parent, or those with parental responsibility, within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, APTCOO may charge a fee to cover the cost of supplying it.

This right applies as long as the child concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

CCTV

APTCOO uses CCTV in various locations around the APTCOO sites to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV and comply with data protection principles.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to **Martin Cope.**

Photographs and videos

As part of our activities, we may take photographs and record images of individuals within APTCOO.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials.

We will clearly explain how the photograph and/or video will be used to both the parent/carer and the child. Where we don't need parental consent, we will clearly explain to the young person themselves how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at APTCOO events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other young people are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

We will obtain written consent from parents/carers, for photographs and videos to be taken of children for communication, marketing and promotional materials.

Where APTCOO takes photographs and videos, uses may include:

- Within APTCOO on notice boards and in APTCOO brochures, newsletters, etc
- Outside of APTCOO by external agencies such as newspapers, campaigns, etc.
- Online on the APTCOO website or social media pages.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way, we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, young people, and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard and their increasing use throughout the world.

APTCOO recognises that AI has many uses to help people learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, APTCOO will treat this as a data breach, and will follow the personal data breach procedure.

Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified Data Protection Lead, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge. APTCOO's Data Protection Lead is **Karen Kilner.**

- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law.

- Completing data protection impact assessments where APTCOO's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the Data Protection Lead will advise on this process)

- Integrating data protection into internal documents including this policy, any related policies and privacy notices.

- Regularly training members of staff on data protection law, this policy, any related policies, and any other data protection matters; we will also keep a record of attendance.

- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.

- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply.

- Maintaining records of our processing activities, including:

    - For the benefit of data subjects, making available the contact details of both APTCOO and the Data Protection Lead, and all information we are required to share about how we use and process their personal data (via our privacy notices).

- For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure.

Personal data breaches

APTCOO will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person.
- The theft of a laptop containing non-encrypted personal data about children.
- Records containing personal information being left in an unsecured area.

Training

All staff, volunteers and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development on a regular basis, and where changes to legislation, guidance or APTCOO's processes make it necessary.

Complaints

Complaints about any aspect of APTCOO's data procedures and practices should be made initially to the CEO who will decide, in consultation with the Chair of the Board of Trustees/Governing Board, 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.

Monitoring arrangements

The Data Protection Lead is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the full Board.

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO)

- On finding or causing a breach or potential breach, the staff member, governor or data processor must immediately notify the Data Protection Lead by emailing them at Karen.kilner@aptcoo.org
- The Data Protection Lead will investigate the report and determine whether a breach has occurred. To decide, the Data Protection Lead will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people

- Staff and governors will co-operate with the investigation (including allowing access to information and responding to questions). The investigation will **not** be treated as a disciplinary investigation.
- If a breach has occurred or it is considered to be likely that is the case, the Data Protection Lead will alert the CEO/headteacher and the chair of the Board of Trustees/Governors.
- The Data Protection Lead will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the Data Protection Lead with this where necessary, and the Data Protection Lead should take external advice when required (e.g., from IT providers) (See actions relevant to specific data types at the end of this procedure).
- The Data Protection Lead will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences.
- The Data Protection Lead will work out whether the breach must be reported to the ICO, and the individuals affected using the ICO's self-assessment tool.
- The Data Protection Lead will document the decisions (regardless of the outcome), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on APTCOO's secure Microsoft 365 software system.
- Where the ICO must be notified, the Data Protection Lead will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113)

within 72 hours of APTCOO's awareness of the breach. As required, the Data Protection Lead will set out:

- A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
- The name and contact details of the Data Protection Lead
- A description of the likely consequences of the personal data breach.
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

- If all the above details are not yet known, the Data Protection Lead will report as much as they can within 72 hours of APTCOO's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the Data Protection Lead expects to have further information. The Data Protection Lead will submit the remaining information as soon as possible.

- Where APTCOO is required to communicate with individuals whose personal data has been breached, the Data Protection Lead will tell them in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach
    - The name and contact details of the Data Protection Lead
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.
- The Data Protection Lead will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- The Data Protection Lead will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).

Records of all breaches will be stored on APTCOO's secure Microsoft 365 system.

- The Data Protection Lead, CEO and headteacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by APTCOO to reduce risks of future breaches.

Actions to minimise the impact of data breaches

We set out below the steps APTCOO might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.

- Members of staff who receive personal data sent in error must alert the sender and the Data Protection Lead as soon as they become aware of the error.

- If the sender is unavailable or cannot recall the email for any reason, the Data Protection Lead will ask the IT & Systems coordinator to attempt to recall it from external recipients and remove it from APTCOO's email system (retaining a copy if required as evidence).

- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the Data Protection Lead will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.

- The Data Protection Lead will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request

- The Data Protection Lead will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

- If safeguarding information is compromised, the Data Protection Lead will inform the designated safeguarding lead and discuss whether APTCOO should inform any, or all, of its local safeguarding partners

- Other types of breach that may take place include:

    - Details of pupil interventions for named children being published on the APTCOO website.
    - Non-anonymised learner exam results or staff pay information being shared with governors.
    - A laptop containing non-encrypted sensitive personal data being stolen or hacked.
    - Hardcopy reports sent to the wrong learners or families.
    - Records showing learner personal information left in an unsecured area.

Contacts

If you have any enquiries in relation to this policy, please contact the Data Protection Lead Karen.kilner@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.

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

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
September 2023	Mike Holmes & Compliance Lead	V3 Update and review	V3 Annual Review. Reformation of sections and relevant updates in line with ICO guidance.
August 2024	Compliance Lead	V4 annual review	V4 annual review – document reformatted, links updated and DPO amended to Data Protection Lead as APTCOO do not meet the ICO requirements for a qualified DPO (Tier 1 charity with small scale data management).