



TEENAGE KICKS

Engagement • Progress • Outcomes

DATA PROTECTION POLICY

Approved by:	James Docherty
Last reviewed on:	29 August 2026
Next review due by:	29 August 2027

Teenage Kicks Limited

2A Partington Street, Failsworth, Manchester, M35 9RD

Tel: 0161 243 3868 Web: www.teenagekicks.uk Email: info@teenagekicks.uk

Headteacher: Mr C Valentine

Data Protection Policy

This policy applies to the whole school and is publicly available on the school website and upon request a copy (which can be made available in large print or other accessible format if required) may be obtained from the School Office.

Monitoring and Review

This policy is subject to ongoing monitoring and will be reviewed at least annually by the Proprietor and Headteacher, and earlier where changes in legislation, regulatory requirements, ICO guidance or school practice make this necessary. Any identified weaknesses will be addressed promptly. The next scheduled review is no later than 29 August 2027. The Data Protection Officer (DPO) for Teenage Kicks is Colin Phillips, who can be contacted on 0161 243 3868 or at colin.phillips@teenagekicks.uk.

1. Definitions

Personal Data Any information relating to an identified, or identifiable, individual. This may include the individual's: Name (including initials) Identification number Location data Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity

Special categories of personal data Personal data which is more sensitive and so needs more protection, including information about an individual's: Racial or ethnic origin Political opinions Religious or philosophical beliefs Trade union membership Genetics Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes Health – physical or mental Sex life or sexual orientation

Processing Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual

Data subject The identified or identifiable individual whose personal data is held or processed.

Data controller A person or organisation that determines the purposes and the means of processing of personal data.

Data processor A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller

Personal data breach A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

2. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, advisers, visitors and other individuals is collected, stored and processed in accordance with the UK GDPR and the Data Protection Act 2018 (DPA 2018). This policy applies to all personal data, regardless of whether it is in paper or electronic format.

3. Legislation and guidance

This policy reflects the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Data (Use and Access) Act 2025, together with current guidance from the Information Commissioner's Office (ICO). It also reflects relevant requirements relating to CCTV and surveillance, biometrics and the handling of data protection complaints.

4. The Data Controller

Teenage Kicks processes personal data relating to parents, pupils, staff, advisers, visitors and others, and therefore is a data controller. The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required. The school's registration number is 00017619143

5. Roles and responsibilities

This policy applies to all staff employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Proprietor

The proprietor has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law and advising on related policies and procedures. At Teenage Kicks the DPO is Colin Phillips. The DPO will report directly to the Proprietor on data protection matters and is a point of contact for individuals whose personal data the school processes and for the ICO. The DPO must be able to perform the role independently and without a conflict of interests.

5.3 Headteacher

The Headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 Staff Responsibilities

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO 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 rely on or capture consent, draft a privacy notice, respond to an individual exercising data protection rights, or make a restricted transfer of personal data outside the UK
- If there has been a data breach – see the Teenage Kicks Data Breach Procedure
- 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

6. Data protection principles

The UK GDPR is based on data protection principles that our school must comply with. 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 in a way that ensures it is appropriately secure
- This policy sets out how the school aims to comply with these principles.

7. Collecting Personal Data

7.1 Lawfulness, Fairness and Transparency

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

- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- The processing is necessary for a task carried out in the public interest or in the exercise of official authority, where this lawful basis applies
- The data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual has given valid consent. Where special category data is processed, the school will also identify an appropriate condition under Article 9 UK GDPR and the Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps which require use of personal data, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services). Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, Minimisation and Accuracy

We will only collect personal data for specified, explicit and legitimate purposes and will explain those purposes through an appropriate privacy notice. If we need to use personal data for a new purpose, we will consider whether the new use is compatible with the original purpose and identify an appropriate lawful basis. Staff must only process personal data where necessary for their role. Personal data will be retained and disposed of in accordance with the school's retention arrangements.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies and have an appropriate lawful basis for doing so; consent will only be sought where consent is the appropriate lawful basis
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.

We may also share personal data with law enforcement agencies, government bodies, local authorities and other organisations where this is required or permitted by law, including for safeguarding, legal proceedings, the prevention or detection of crime, taxation and other statutory functions.

- Only share the personal data that the supplier or contractor needs to provide the service, and ensure that appropriate contractual and security arrangements are in place.
- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations

We may share personal data with emergency services and local authorities where necessary to respond to an emergency affecting pupils or staff. Restricted transfers of personal data outside the UK will only take place where the requirements of UK data protection law are met.

- Research and statistical purposes where an appropriate lawful basis and safeguards are in place, including anonymisation where appropriate.

9. Subject Access Requests and Other Rights of Individuals

9.1 Subject Access Requests

Individuals have the right to make a subject access request (SAR) for access to their personal data. A SAR may be made verbally or in writing and does not need to use particular wording.

- 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
 - The source of the data, if not the individual

Anyone receiving a subject access request must forward it to the DPO promptly. The school may ask for information reasonably necessary to identify the requester or clarify the scope of the request.

- Whether automated decision-making is being applied to their data and, where required, meaningful information about the logic involved and the significance and envisaged consequences of the processing.
- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested If staff receive a subject access request they must immediately forward it to the DPO.

9.2 Children and Subject Access Requests

The right of access belongs to the pupil. A parent/carer may make a request on a pupil's behalf where the pupil authorises them to do so or where the pupil is not competent to exercise the right independently. The school will consider the pupil's maturity, understanding and circumstances on a case-by-case basis and will take account of safeguarding and confidentiality considerations.

When responding to requests, we

- May request proportionate evidence of identity where there are reasonable doubts about the requester's identity
- May seek reasonable clarification where this is necessary to identify the information requested
- Will respond without undue delay and normally within one month of receipt of the request, subject to the rules on when the time limit begins
- Will provide the information free of charge
- May extend the response period by up to two further months where a request is complex or where the individual has made multiple requests, and will inform the individual of any extension and the reasons for it within the initial one-month period

We will not disclose information if it

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is information to which a statutory exemption or restriction applies. Where a request is manifestly unfounded or excessive, the school may refuse to act or may charge a reasonable fee where permitted by law. The school will explain the reasons and the individual's right to complain to the ICO.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.3 Other Data Protection Rights of the Individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), 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, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request information about safeguards used for restricted transfers of their personal data outside the UK
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to another organisation in a structured, commonly used and machine-readable format where the right to data portability applies. Requests to exercise data protection rights should be sent to the DPO. Staff who receive such a request must forward it to the DPO promptly.

10. Requests for pupil information

As an independent school in England, Teenage Kicks is not subject to the parental right of access to educational records under the Education (Pupil Information) (England) Regulations 2005. Access to a pupil's personal data is instead considered under data protection law. The right of access belongs to the pupil, although a parent/carers may exercise that right on the pupil's behalf where appropriate, as explained in section 9.2.

11. CCTV

Please refer to the school's CCTV policy for information.

12. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school. We will obtain written consent from parents/carers for photographs and videos to be taken of pupils for communication, marketing and promotional materials. Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carers and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used. Uses may include:

- Within school on notice boards, school posters, prospectus and newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns

- Online on our school website or social media pages. Where consent is the lawful basis, consent may be refused or withdrawn at any time. Withdrawal of consent does not affect processing that was lawful before withdrawal. Images taken for safeguarding, evidential, educational or other purposes may be processed on another lawful basis where appropriate. We will avoid publishing unnecessary identifying information alongside promotional images of pupils.

13. Data protection by design and default

We will integrate data protection into new and existing processing activities and systems, taking account of the nature, scope, context and purposes of processing and the risks to individuals.

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- 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 (see section 6)
- Completing data protection impact assessments (DPIAs) where processing is likely to result in a high risk to the rights and freedoms of individuals, including where required when introducing new technologies
- Integrating data protection into internal policies, procedures and privacy notices, and providing regular staff training on data protection responsibilities
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
- For the benefit of data subjects, making available the name and contact details of our school and DPO 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, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off-site it must be safeguarded; papers should be carried in locked briefcases. The use by staff of removable media e.g. USB sticks is not permitted.
- School systems and devices will use appropriate authentication controls, including strong passwords and multi-factor authentication where appropriate. Staff must follow the school's security requirements and must not store school personal data on personal devices unless this has been specifically authorised and secured.

- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

15. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16. Personal data breaches

The school will take appropriate technical and organisational measures to reduce the risk of personal data breaches. Suspected or actual breaches must be reported to the DPO immediately. Where a breach is likely to result in a risk to individuals' rights and freedoms, the school will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it. Where a breach is likely to result in a high risk, affected individuals will also be informed without undue delay unless an exception applies.

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing personal data about pupils

17. Training

All staff are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

18. Data protection complaints

Individuals may raise a complaint about the school's handling of their personal data with the DPO. The school will provide a clear means of making a complaint, acknowledge a data protection complaint within 30 days, investigate it appropriately without undue delay and communicate the outcome promptly, in accordance with section 164A of the Data Protection Act 2018. Individuals also have the right to complain to the ICO.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy. It will be reviewed at least annually, and sooner where legislation, regulatory requirements or school practice changes. The reviewed policy will be shared with the Proprietor.

20. Links with other policies

This Data Protection Policy should be read alongside the following documents:

- Online Safety Policy
- Student ICT Acceptable Use Agreement

-
- Safeguarding and Child Protection Policy
 - CCTV Policy