Data Protection and Privacy Policy Statement

Reviewer:	Michael Kaoura
Position:	Business Development and Compliance Manager (Data Protection Officer)
Date Last Reviewed:	24th November 2024
Review Date:	24th November 2026

Contents

1.Monitoring and Review

The Data Protection Officer will undertake a review of the policy for the purpose of monitoring, by no more than 2 years of the from the date of last review, or earlier if there are significant changes to systems or process within Oak Activities or, if legislation, regulatory requirements or best practice guidelines should require.

2. Legislation

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020 Data Protection Act 2018 (DPA 2018)

This policy also has regard to the following guidance:

'Guide to the UK General Data Protection Regulation (UK GDPR)'

ICO (2012) 'IT asset disposal for organisations'

DfE (2023) 'Data protection in schools'

ICO's guidance for the use of surveillance cameras and personal information.

3.Terminolgy

Personal Information/Personal Data	Personal information is any information about any living person from which they can be identified. This can be on paper, on a computer or even just talked about. Personal information can relate to, for example, past or present employees/workers, contractor/suppliers, patients, service users, residents, customers or shareholders. Some examples are: personal contact details, such as name, address, email, telephone number, date of birth, bank account details.

Special Category of Personal Information/Sensitive Personal Information	Information about an individual's racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; health; sex life or sexual orientation; criminal convictions, offences or alleged offences; genetic data; or biometric data for the purpose of uniquely identifying an individual.
Processing	Any activity that involves using personal information. This includes collecting personal information, recording it, storing it, retrieving it, using it, amending it, disclosing it, destroying it, and transferring it to third parties.
Data Protection Impact Assessment	A data protection impact assessment is an assessment of the impact on individuals of the envisaged processing operations on the use of their personal data.
Direct Marketing	Direct marketing means the communication (by whatever means) of advertising or marketing material which is directed to particular individuals.
Data controller	An organisation or person, that determines the way that personal data is processed or managed e.g. A Local Authority.
Data Processor	A person, or other body that processes data on behalf of the data controller.
Data Protection Officer	Nominated person responsible for overseeing and monitoring the compliance of their organisations processes in compliance with Uk data protection law. They must have the training, knowledge and authority to do so effectively.

Individual/Data Subject	The person whose individual data is held by the company.
Regulatory Authority	This definition refers to the regulatory body e.g. Information Commissioners Office, responsible for regulating and inspecting all practice relating to information governance.
Commissioning Body	The local authority/school/academy responsible for placing the student or commissioning the provision.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.

4.Data protection principles

Oak Activities sets out within this policy the way in which the company will comply with UK GDPR and the principles set out in the law. The principles set out by the law are that data is:

- Accurate and kept up to date;
- Adequate, relevant and limited to what is necessary and required by the company;
- Collected for clear, explicit and legitimate purposes, and processed in line with those purposes;
- Held for no longer than is required and for legitimate purposes relating to why it is processed;
- Processed in a lawful, fair and transparent manner;
- Secure when processed and stored in a secure way to protect against, unlawful or unauthorized processing and against accidental loss, destruction or damage.
- The processing is necessary for the establishment, exercise or defense of legal claims

5.Introduction

Oak Activities is committed to all aspects of data protection and it takes its duties seriously under the Data Protection Act 2018 and the General Data Protection Regulations (UK GDPR).

The company processes personal data relating to parents, students, and staff. Our Data Protection and Privacy Policy statement is to confirm your privacy rights and how the law protects you.

Types of data Oak Activities may hold information about:

- Current, past and prospective employees;
- Current, past and prospective students;

- Individual staff members of commission bodies;
- stakeholders, parents, foster carers and all other prospective parties of which the company communicates with.

Oak Activities is registered as a data controller with the ICO and will ensure that its registration is renewed annually. The company appoints a data protection officer (DPO) who has the responsibility for overseeing, reviewing and implementing the policy to comply with UK/EU data protection laws.

The Data Protection Officer will report annually to the Oak activities senior management board and have regular correspondence on all data protection matters with the Managing Director Tom Milner.

6.Roles and Responsibilities

The DPO for Oak Activities is Michael Kaoura (Business Development and Compliance Manager) and is contactable via Michael.kaoura@oakactivities.com. The role of the DPO is to act as first point of contact for data subjects whose data Oak Activities processes, and for the ICO.

Operations Managers and Alternative Provision Managers act as the representative of the data controller on a day to day basis.

All Employees of Oak Activities are responsible for informing the company to any changes to their personal data in accordance with the policy. All changes to their personal data including, changes of address, next of kin and contact information must be shared.

All employees must contact the DPO in the circumstance below:

- If they are concerned that policy is not being followed;
- If there has been a data breach identified
- If they require support around contracts, tendering or, sharing personal data with third parties
- If they unsure whether they have basis to use personal data for a specific purpose
- If they undertake any direct marketing activity to individuals (including electronic marketing by email, telephone, fax or text message);
- Implement significant changes to systems or the business (including new or different technology) which involve processing personal information.
- When dealing with data protection rights raised by data subjects, in the process of capturing consent, transferring personal data outside borders, or drafting a privacy notice;
- With any queries or questions pertaining to data protection legislation/law, operations of the policy, retaining personal data, or keeping personal data secure;
- When engaging with new processes that may impact on privacy rights of data subjects.

Failure to observe the data protection principles within this policy may result in an Employee incurring personal criminal liability. It may also result in disciplinary action up to and including dismissal. For example, if an employee accesses another employee's employment records without the requisite authority, Oak Activities will treat this as gross misconduct and instigate its disciplinary procedures. Such gross misconduct will also constitute a criminal offence.

7.Lawful basis for processing information

Oak activities will only process personal data based on one of the legal bases set out below:

- The data subject has given consent;
- To meet legal compliance, for example safeguarding children;
- To protect a data subjects vital interests e.g. life or death scenarios
- The processing of data is necessary for the performance of the contract with the data subject;
- To perform a task in the public interest or for official functions where the task or function has a clear basis in law e.g. LADO investigation;
- The process is vital for performance of contractual arrangement between data subject and employer e.g. where the data subject has requested the company take specifics steps before entering into a contractual agreement e.g. obtaining employment references.

7.1 Special Category Personal Data

Under data protection law special Oak Activities will only process special categories of personal data if:

- The data subject (or parent/carer when appropriate) has given explicit consent.
- The data needs to processed in order to exercise obligations or rights in relation to employment, social security or social protection law.
- The data subject is incapable of giving consent, and the processing is necessary to protect vital interests.
- The data has already been manifested publicly by the data subject.
- The processing is necessary for the establishment, exercise or defense of legal claims.
- The data needs to be processed for reasons of substantial public interest as defined in legislation.
- The processing is required for the purpose of medical treatment undertaken by health professionals, including assessing the working capacity of employees and the management of health or social care systems and services.
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law

Oak Activities 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 through our referral process.

In the rare occasion that company wants to use personal data for reasons other than those given when we first obtained it, we will inform the data subjects concerned before we do so and seek consent where necessary with a clear opt in process. Staff must only process personal data where it is necessary to do their jobs.

8.Consent

Consent is defined in UK GDPR Article 4(110 as: *'' any freely given, specific, informed and inambiguous 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''.*

Oak Activities will ensure that:

- It aims to give data subjects choice and control how their data is used, if the individual has no choice, consent is not freely given and it will be invalid.
- It will provide data subjects clear explanation of the data processing to which they are consenting. The company will provide clear opt in to this consent and it will be voluntary and freely given.
- It will always aim to gain consent from the data subjects themselves and not a third party, (other than in specific cases where there authorization, such as power of attorney). Where the individual lacks the capacity to consent, a 'best interest' assessment must be undertaken to inform the decision making process.
- That consent is kept up to date and will be re-sought on an annual basis to ensure validity is maintained.
- Will only obtain an individual's consent where there is genuine choice and genuine control by the individual whether or not to consent to the processing of their personal information. We will rely on other legal bases where they are appropriate for the processing.
- Personal data or photographs will not be used in newsletters, websites or other media without the consent of the data subject. We will seek consent before displaying within our Locations, personal information about individuals (including, certificates/qualifications). Routine consents will be incorporated into the Location's individual's care data gathering sheets to avoid the need for frequent, similar requests for consent being made by the Location.
- All individuals must be given the opportunity to opt-in to receive material at the point of data collection. The appropriate opt-in mechanisms must be put in place where third party marketing or advertising materials are distributed to named individuals. In situations where this cannot be feasibly done, the materials must not be distributed.

9. Direct Marketing

Direct marketing is defined in section 122(5) of the Data Protection Act 2018 as: ''the communication (by whatever means) of advertising or marketing material which is directed to particular individuals.

Oak Activities will not:

- Sell your data to a third party. **Y**our collected data may help us, as a business of educational support and tutoring services, to study how our clients, tutors, users of our website and others who make enquiries, utilise our products and services and to improve the services that we provide.
- Participate in direct marketing practices without gaining explicit consent or having a legitimate business reason.

10. Sharing personal data

Oak Activities will only share personal data in rare circumstances. Circumstances where we may share personal data are:

- Where we need to liaise with other agencies, e.g. for safeguarding reasons or LADO investigations.
- There is a issue that compromises the safety of students and staff due to an issue with a student or parent.
- We procure a data management system to enable us to run our business more efficiently. In these circumstances Oak Activities will only appoint other data processors that comply with UK data protection law , there is a clear data sharing agreement in place and that, only necessary information is shared to enable them to carry out the terms of their contract.
- Where we are required to by law enforcement of government bodies.
- Where local authorities or emergency services need to respond to an emergency that impacts the safety of the public, staff or students.

11. Subject to access requests

Data subjects have the right to make a 'subject to access request' to gain access to any personal data or correspondence that Oak Activities holds about them, which includes:

- The right to be informed as to information we collect, and how we hold and handle it
- The right to access a copy of any data held
- The purpose of processing
- The categories of data concerned
- The right to rectification of their personal data
- The right to be informed who it has or will be shared with
- The right to lodge a compliant with the ICO
- The right to request erasure of personal data
- The right to request restriction of processing personal data
- The right to transfer their data to any other person, or organsiation
- The right not to be subject to any automated decision making about using personal data or profiling data subjects

These rights are subject to certain exemptions which are set out in the General Data Protection Regulations (UK GDPR) and Data Protection Act 2018. Therefore, requests from individuals regarding their personal information must be handled in line with the Access to Records policy (GIG 08); and advice must be sought from the Data Protection Officer.

All enquiries about the handling of personal information must be dealt with promptly and courteously.

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

- 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.

11.1 Children and subject to 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 subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Communications aimed towards children and young people must be clear and concise. It should be age-appropriate and presented in a way that appeals to a young audience.

Where we rely on consent as the lawful basis for processing information about children and young people we will ensure that we obtain consent from children aged 13 years and over.

For children under this age we will seek consent from whoever holds parental responsibility for the child. Where parents have separated or the young person lacks the capacity to consent, consideration should be given to the 'best interests' of the child/young person.

Children aged 12 and above are generally regarded as being mature enough to understand their rights and the implications of a subject to access request. Therefore, a number of subject to access request to Oak Activities may not be granted without gaining permission of the pupil. All pupil's ability to understand their rights will be judge on a case by case basis.

11.2. Responding to subject to access requests

When responding to requests Oak Activities:

- May ask for 2 forms of identification
- may contact the individual via phone or ask to meet in person to confirm the request was made
- will respond without delay within a 30 day period from when receipt of the request was received or (where confirmation of identification was received)
- may need further time to comply with the request if the request are multiple and complex. In these circumstances the maximum response time will be 3 months and the data subject will be informed within 1 month of the request, should additional time be needed for the response

Reasons to restrict or decline data access request:

- information is part of sensitive documents, such as those relating to crime, immigration, legal proceedings or legal professional privilege, management forecasts negotiations, confidential references

- might cause serious harm to the mental and physical wellbeing of a pupil or another individual
- would reveal a circumstance where a child or family member is or has been abused, or is at risk of abuse and the disclosure of the information would bot be in the best interest of the child or family member
- would disclose another data subjects personal data that cannot be anonymized, and without that data subjects consent

Any refusals to allow access to data will be explained and data subjects will be offered the right to complain to the ICO or they can enforce a request through legal measures.

If it is deemed that requests are unfounded or excessive, we may refuse to act. We will consider each requests on its own merit.

12. Data security and Retention

Oak Activities staff are responsible for ensuring that:

- any personal data which they have access to is always kept securely;
- personal information is not disclosed either verbally or in writing or otherwise to any unauthorised third party with consent;
- computer workstations in administrative areas are securely positioned so that they are not visible to casual observers and are not left unattended when the user is still logged-on or in any other circumstances when the personal details of staff or individuals in our care could be accessed by unauthorised persons;
- paper files containing personal information are kept to a minimum and are stored where they are not accessible to anyone who does not have legitimate reason to view or process them and they are not left on view in circumstances in which they could be read by unauthorised persons;
- 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;
- particular care and measures are taken to protect sensitive personal information from unauthorised access.

Oak Activities Management team are ultimately responsible for ensuring that data is restricted internally to only those staff member or should and need access to enable them to carry out their role effectively.

13. Disposal of records

All staff are responsible to ensure that data is not retained for longer than it should be. Any data that is out of date, inaccurate or no longer needed will be disposed of securely.

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.

14. Data Security and Removal of Records from Oak Activities Premises

Only in these circumstances may a member of Oak Activities staff remove data subjects records from an Oak Activities premises:

- When a pupil is moving to another provision or back into a mainstream setting.
- Where personal information needs to be taken off site, staff must sign it in and out from the academy office
- 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
- 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
- Passwords that are at least 10 characters long containing letters and numbers are used to access academy computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Paper-based records containing confidential information must never be left on office or classroom desks, on staffroom tables, pinned to notice/display boards or left anywhere else where there is general access

15.Bring Your Own Device guidance

Typically this relates to smart phones, tablets and USB memory sticks.

Data stored by the Oak Activities should never be transferred to a personal device unless the device is protected by a password (encryption is required if the data relates to information that would identify an individual) and permission for the transfer has been given by the Oak Activities Data Protection Officer. Agreement must be reached as to how long the data may remain on the device. This will only be done in exceptional, mutually agreed, circumstances where complete security and encryption are guaranteed.

When transferring data from personal devices ensure you are using a secure channel. Public wi-fi networks may not be secure. Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices

Staff, pupils or board members who store personal information on their personal devices are expected to follow the same security procedures as for Oak Activities owned equipment.

16. Personal data breaches

Oak Activities will make all reasonable endeavors 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. Such breaches in an Oak Activities context may include, but are not limited to:

- safeguarding information being made available to an unauthorised person
- the theft of an Oak Activities laptop/phone containing non-encrypted personal data about pupils
- the disclosure of any personal information to an email recipient by mistake

17.Safeguarding

Oak Activities abides by the guidelines of UK GDPR regulations to ensure that it is compliant with UK data protection law. These guidelines do not prevent or limit the sharing information to enable Oak Activities to safeguard its pupils.

Oak Activities managers and Data Protection Officer have due regard for the safety and well-being of staff, pupils and family members of our pupils and in these circumstances will share information in order not obstruct any safeguarding or legal procedures.

The Management Board will ensure staff are:

- Confident of the processing conditions which enable Oak Activities to store and share information for safeguarding purposes, including information which may be deemed personal; and sensitive and could be considered as 'special category data'.
- Be confident that information can be shared without consent where safeguarding or legal or reasons, and that sharing of the information will ensure the safety of pupils in time effective manner.

Oak Activities will ensure that information shared with relevant individual individuals or agencies enables them to identify, assess and respond to risks or concerns about safeguarding as soon as reasonably possible. DSL's for Oak Activities should always record data that has been shared in relation to safeguarding to eliminate any doubt they should record the following:

- What data has been shared
- With whom it was shared
- The reason the data was shared
- Whether Oak Activities obtained consent from parents or data subjects
- If no consent was sought, what the rationale was behind this

Oak Activities will always aim to gain consent to share information; however in instances where it would either delay protections of a family or child or place them at further risk the company will decide to gain consent at its own discretion

Oak Activities will always aim to get consent to share information where it is deemed appropriate; however staff will not hesitate to share information where it would compromise.

18.Training

All Oak Activities staff are requested to complete mandatory data protection training as part of their induction process.

The topic also form part of all staffs continual professional development. It is down to Oak Activities Operations Managers to ensure that AP Managers are prompting their staff to complete this annually. The Data Protection Officer for the company completes annual checks to ensure that staff are all trained.

In rare the event of a data breach staff may be requested to complete training or revisit as part of the companies response to the incident.

19.Photgraphs and videos

As part of our daily activities Oak Activities staff may request to take photo's or videos of individuals that access our provision.

Consent for such activities is obtained as part of the Oak Activities onboarding process from parents/carers.

Oak Activities clearly explains that any videos or photos taken are utilised for communication, marketing or promotional reasons and will normally only be shared on:

- Oak Activities social media;
- websites and with;
- commissioning bodies to share the good work a pupil has achieved at the provision.

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

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with 10 other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Consent can be refused at any point during a pupils time attending our provision. If consent is withdrawn the company will delete the photograph or video and remove from all Oak Activities marketing.

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. We provide our staff with guidelines on the use of images within the staff code of conduct and online safety policy.

20. Links with other policies

This data protection policy is linked to our:

- Online Safety Police

- Safeguarding and Child Protection
- Staff Code of Conduct
- Onboarding/Referral process
- GDPR/Privacy notice for staff, pupils and candidates

Appendix 1:Personal data breach procedure

Oak Activities endeavors to ensure that its following guidelines of managing data breaches set out and produced by the ICO Personal data breaches: a guide | ICO

- On identification of a data breach all Oak Activities staff members or, data processors must immediately notify the DPO Michael.kaoura@oakactivities.com
- The DPO will initiate the investigation process , and determine whether a breach has occurred. The process that follows is to identify whether the breach has been accidental or unlawful and has either been:
  - Lost
  - Stolen
  - Destroyed
  - Altered
  - Disclosed or made available where it should not have been
  - Made available to unauthorized people
- The DPO will alert the Managing Director Tom.milner@oakactivities.com
- The process is then to ensure that minimal impact is caused by the breach, the DPO will be assisted by nominated and relevant staff members or data processors where necessary.
- Consequences of the data breach will then be assessed by the DPO to determine severity and how likely they are to happen
- The DPO will the assess as to whether the breach must be reported to the ICO. This will be judge case by case and must be judge on whether the impact will negatively affect people's rights and freedom's, cause them physical harm or material or non-material damage (e.g. emotional distress) through but not limited
  - Damage to reputation
  - Discrimination
  - Financial loss
  - Identity theft or fraud
  - Loss of confidentiality
  - Loss of control over their data
  - Unauthorized reversal of pseudonymization (e.g, key coding)
  - Any other significant economic or social disadvantage to data subjects concerned

In the unlikely event that any of the above have been breached the DPO must notify the ICO via their Report a breach | ICO page within 72 hours. These are the timeframes set out by the ICO.

In the event of a breach that needs to be reported to the ICO the DPO must:

- Set out a description of the nature of the data breach including, the categories and the amount of data subjects impacted.
- The amount of data records concerned
- Name and contact details of the DPO

- A description of the potential consequences of the data breach
- Provide information of what measures have already been taken
- What further measures need to be taken, and mitigation on what, if any, adverse effects on data subjects concerned

- The DPO may not have all of the above information at point of reporting to the ICO and therefore, will report as much information as has been gathered. The DPO will explain rationale as why and when they will obtain all the relevant information and submit as soon as possible.
- The DPO will notify any third parties, e.g. commissioning bodies, police, insurers, banks who may be able to help in mitigation in the loss to individuals.
- The DPO's role is to assess the individual risk to data subjects, based on severity and likely impact/ risk. If risk of serious impact is high then a process will be set to inform all individuals involved in writing. The notification will set out:
  - The name and contact of the DPO for Oak Activities
  - Description as to the likely consequences of any breach
  - Anthe measures that have or, will be taken to reduce risk, prevent further breach and mitigate any damage on individuals concerned
- An accurate documentation will be taken and recorded of each breach by the DPO, the record will include:
  - Facts, cause and effects
  - Action taken to control/contain
  - Further robust planning to mitigate any further risk
- The DPO and Managing director will meet to review each data breach and how assess how it can be prevented in the future.
- All data breaches records will be stored with the DPO in secured digital folders with the central management team.

Actions to minimize the impact of data breaches will be reviewed regularly and shared to ensure that any potential risk of pf breaching personal or sensitive information is limited and mitigated as much as possible.

Safeguarding or sensitive information being disclosed via email

- If special category data is made available via email the sender must attempt to recall the information as soon as they become aware and inform their line manager or the DPO.
- If the sender is unavailable and other Oak Activities staff become aware of the data breach then the DPO will ask the ICT department (Evolve) to recall it.
- In any cases where the recall is unsuccessful, the DPO will 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 DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.
- The DPO 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