GDPR

Introductory Statement

Educare11plus needs to hold and to process large amounts of personal data about its students, employees, applicants, contractors and other individuals in order to carry out its business and administrative functions.

By personal data, Educare11plus refers to any information relating to an identified or identifiable natural person (data subject) who can be identified, directly or indirectly by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.
This policy is intended to ensure that personal data is dealt with properly and securely and in accordance with General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA).

GDPR and DPA are the laws that protect personal privacy and upholds individual's rights. These laws were set to strengthen and unify all data held within an organisation. It explains what kind of information teachers should keep, how to obtain and store this information and how long it should be kept. GDPR and DPA applies to anyone who handles or has access to people's personal data.
This policy will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

Policy Objectives

Educare11plus aims to help children and seeks to enable each student to develop his/her full potential. Part of our mission is to provide a safe and secure environment for learning and encourage children to develop positive attitude and respect for themselves and others. Complying with its obligations under the GDPR and DPA, the Children's Act 1989, the Childcare Act 2006, and all other relevant legislation is a fundamental aspect of its mission.

Educare11plus is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rights under the legislation.
Educare11plus supports that a Data Subject is a living, identified or identifiable individual about whom we hold personal data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

All staff must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this policy.

This policy aims to

Ensure that Educare11plus complies with its obligations under the GDPR and DPA.

Ensure that the data protection rights of students, staff and other members of the Educare11plus are safeguarded.

Scope of the Policy

This policy applies to the keeping and processing of personal data, both in manual form and on computer, including personal data held on both staff and pupils.

GDPR Article 4 defines Personal data as any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information. The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual. This includes any expression of opinion about an individual and intentions towards an individual. Under the GDPR personal information also includes an identifier such as a name, an identification number, location data or an online identifier.

Educare11plus collects a large amount of personal data every year including: pupil records, staff records, names and addresses of those making enquiries, examination marks, references, fee collection as well as the many different types of research data used by Educare11plus. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of law enforcement agencies, government agencies and other bodies.

The policy applies to all staff, the board of management, parents/guardians, pupils and others insofar as the measures under the policy relate to them. The policy also applies to all locations from which personal data is accessed including off-campus.

Contents of the Policy

The policy content is divided into two sections as follows:

Section A:

Details of all personal data which will be held, the format in which it will be held and the purpose(s) for collecting the data in each case.

Section B:

Details of the arrangements in place to ensure compliance with the principles set out in the GDPR.

Section A:

Details of all personal data which will be held, the format in which it will be held and the purpose(s) for collecting the data in each case.
Personal data is subject to the legal safeguards specified in the GDPR.

Staff records:

These may include:

• personal information (such as name, employee or teacher number, national insurance number)
• characteristics information (such as gender, age, ethnic group)
• original records of application, appointment and contract information (such as start date, hours worked, post, roles and salary information)
• work absence information (such as number of absences and reasons, career breaks, parental leave, study leave)
• work record, qualifications (and, where relevant, subjects taught)
• relevant medical information
• addresses
• other relevant payroll information
• record of appointments to promotion posts
• details of complaints and/or grievances including consultations or competency discussions, action/improvement/evaluation plans and record of progress.

Storage Format

The format in which the above records will be kept will be either manual record (personal file within filing system), computer record (database) or both. They will be kept securely in accordance with the Educare11plus's data protection obligations.

Purpose for keeping staff records

At Educare11plus, Staff data is essential for operational use and facilitate other administrative tasks.
Student records

These may include:
• information which may be sought and recorded at enrolment, personal identifiers and contacts (name, address, email address, phone number, unique pupil number)
• names and addresses of parents/guardians and their contact details
• age, date of birth, sex, sexual orientation, marital status, family status
• characteristics (race, language, nationality, ethnicity, origin, colour, religious or political beliefs or associations)
• national insurance numbers, national health service numbers
• safeguarding information (such as court orders and professional involvement)

• special educational needs (including the needs and ranking)
• medical and administration (such as doctors' information, pupil health, dental health, allergies, health care history including information on physical/mental disability, medication and dietary requirements)
• attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended)
• assessment and attainment (such as school work, marks and exam results, courses enrolled for and any educational related results)
• Behavioural information (such as attendance, exclusions and any relevant alternative provision put in place)
• Trips and activities, catering management
• Identity management and authentication
• Staff development reviews
• Information on previous academic record

Storage Format

The format in which the above records will be kept will be either manual record (personal file within filing system), computer record (database) or both. They will be kept securely in accordance with the Educare11plus's data protection obligations.

Purpose for keeping student records

At Educare11plus, student data is essential to enable each student to develop his/her full potential, to comply with legislative or administrative requirements, to ensure that eligible students can benefit from the relevant additional teaching or financial supports, to support the provision of religious instruction, to enable parent/guardians to be contacted in the case of emergency.

Board of Management records

These may include:

• Name, address and contact details of each member of the board of management
• Records in relation to appointments to the board
• Minutes of board of management meetings and correspondence to the board which may include references to particular individuals

Storage Format

The format in which the above records will be kept will be either manual record (personal file within filing system), computer record (database) or both. They will be kept securely in accordance with the Educare11plus's data protection obligations.

Purpose for keeping Board of Management records

At Educare11plus, Board of Management details essential to record board appointments and document decisions made by the board.

Section B

Details of the arrangements in place to ensure compliance with the principles set out in the GDPR.

This policy sets down the arrangements in place to ensure that all personal data records held by Educare11plus are obtained, processed, used and retained in accordance with the following principles set out in the GDPR:

Lawfulness, Fairness and Transparency

- Personal data must be processed lawfully, fairly and in a transparent manner

Purpose Limitation

- Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Personal data must not be used for new, different or incompatible purposes from that disclosed when it was first obtained unless the data subject has been informed of the new purposes and they have consented where necessary.

Data Minimisation

- Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed
- Staff may only process data when their role requires it. Staff must not process personal data for any reason unrelated to their role.
- Educare11plus maintains a Retention Schedule to ensure personal data is deleted after a reasonable time for the purpose for which it was being held, unless a law requires such data to be kept for a minimum time.
- Staff must take all reasonable steps to destroy or delete all personal data that is held in its systems when it is no longer required in accordance with the Schedule.
- Staff must ensure that data subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

Accuracy

Personal data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.

Storage Limitation

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed

Integrity and Confidentiality

Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal information is processed in a manner that ensures appropriate security of the personal data and protects against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

A student aged between 12 and 16 would be required to give consent themselves and, in addition, consent should also be obtained from the student's parent or guardian. In the case of students under the age of twelve consent of a parent or guardian will suffice. Individuals aged 18 or older may give consent themselves.

Transfer Limitation

In addition, personal data shall not be transferred to a country outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data as determined by the European Commission or where the organisation receiving the data has provided adequate safeguards.
Processing means anything done with personal data, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, use, disclosure, dissemination or otherwise making available, restriction, erasure or destruction. These may be provided by a legally binding agreement between public authorities or bodies, standard data protection clauses provided by the ICO or certification under an approved mechanism.

This means that individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. It may also be possible to transfer data where the data subject has provided explicit consent or for other limited reasons. Staff should contact the DPO if they require further assistance with a proposed transfer of personal data outside of the EEA.

Lawful Basis for processing personal information

Before any processing activity starts for the first time, and then regularly afterwards, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing must be selected:

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in Educare11plus.
- Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which Educare11plus is subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the purposes of the legitimate interests pursued by Educare11plus or by a third party.

- The data subject has given consent to the processing of his or her data for one or more specific purposes. Agreement must be indicated clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, the consent must be kept separate from those other matters.

  Withdrawal of consent

  Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be reviewed if personal data is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first gave consent.

  The decision as to which lawful basis applies must be documented, to demonstrate compliance with the data protection principles and include information about both the purposes of the processing and the lawful basis for it in Educare11plus's relevant privacy notice(s).

  Sensitive Personal Information

  Processing of sensitive personal information (known as 'special categories of personal data') is prohibited in line with Article 9 of GDPR unless a lawful special condition for processing is identified.

  Sensitive personal information is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data and personal data relating to criminal offences and convictions, which uniquely identifies a natural person.

  Sensitive personal information will only be processed if:

- There is a lawful basis for doing so as identified on previous page
- One of the special conditions for processing sensitive personal information applies:
- the individual ('data subject') has given explicit consent (which has been clearly explained in a Privacy Notice)
- the processing is necessary for the purposes of exercising the employment law rights or obligations of Educare11plusor the data subject
- the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent
- the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim
- the processing relates to personal data which are manifestly made public by the data subject
- the processing is necessary for the establishment, exercise or defence of legal claims
- the processing is necessary for reasons of substantial public interest

- the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services
- the processing is necessary for reasons of public interest in the area of public health.

Educare11plus privacy notice(s) set out the types of sensitive personal information that it processes, what it is used for, the lawful basis for the processing and the special condition that applies.

Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

Unless Educare11plus can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data. Evidence of consent will need to be captured and recorded so that Educare11plus can demonstrate compliance with the GDPR.

Automated Decision Making

Where Educare11plus carries out automated decision making (including profiling) it must meet all the principles and have a lawful basis for the processing. Explicit consent will usually be required for automated decision making (unless it is authorised by law or it is necessary for the performance of or entering into a contract).

Additional safeguards and restrictions apply in the case of solely automated decision-making, including profiling. Educare11plus must as soon as reasonably possibly notify the data subject in writing that a decision has been taken based on solely automated processing and that the data subject may request Educare11plus to reconsider or take a new decision. If such a request is received staff must contact the Data Protection Officer as Educare11plus must reply within 21 days. Contact details are below:

Data Protection Officer
Educare11plus Ltd
Southern House, Mauldeth Road West, Chorlton Cum Hardy
Manchester. M21 7SP
Email: info@educare11plus.co.uk

Data Protection Impact Assessments

Educare11plus's processes must embed privacy considerations and incorporate appropriate technical and organisational measures in an effective manner to ensure compliance with data privacy principles.

Documentation and records

Written records of processing activities must be kept and recorded including:

- the name(s) and details of individuals or roles that carry out the processing
- the purposes of the processing
- a description of the categories of individuals and categories of

personal data

- categories of recipients of personal data
- details of transfers to third countries, including documentation of the transfer mechanism safeguards in place
- retention schedules
- a description of technical and organisational security measures.
- As part of Educare11plus's record of processing activities, the Data Protection Officer will document, or link to documentation on:
- information required for privacy notices
- records of consent
- controller-processor contracts
- the location of personal information
- Data Protection Impact Assessments
- Records of data breaches.
- Records of processing of sensitive information are kept on:
- The relevant purposes for which the processing takes place, including why it is necessary for that purpose
- The lawful basis for our processing and
- Whether the personal information is retained or erased in accordance with the Retention Schedule and, if not, the reasons for not following the policy.
- Educare11plus will conduct regular reviews of the personal information it processes and update its documentation accordingly. This may include:
- Carrying out information audits to find out what personal information is held
- Talking to staff about their processing activities
- Reviewing policies, procedures, contracts and agreements to address retention, security and data sharing.

Privacy Notice

Educare11plus will issue privacy notices as required, informing data subjects (or their parents, depending on age of the pupil, if about pupil information) about the personal information that it collects and holds relating to individual data subjects, how individuals can expect their personal information to be used and for what purposes.
When information is collected directly from data subjects, including for HR or employment purposes, the data subject shall be given all the information required by the GDPR including the identity of the

DPO, how and why Educare11plus will use, process, disclose, protect and retain that personal data through a privacy notice (which must be presented when the data subject first provides the data).
When information is collected indirectly (for example from a third party or publicly available source) the data subject must be provided with all the information required by the GDPR as soon as possible after collecting or receiving the data. Educare11plus must also check that the data was collected by the third party in accordance with the GDPR and on a basis which is consistent with the proposed processing of the personal data.

Educare11plus will issue a minimum of two privacy notices, one for pupil information, and one for workforce information, and these will be reviewed in line with any statutory or contractual changes.

Individual Rights

Staff as well as any other 'data subjects' have the following rights in relation to their personal information:

- To be informed about how, why and on what basis that information is processed
- To obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a subject access request
- To have data corrected if it is inaccurate or incomplete
- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten')
- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased) or where Educare11plus no longer need the personal information, but you require the data to establish, exercise or defend a legal claim
- To restrict the processing of personal information temporarily where you do not think it is accurate (and Educare11plus is verifying whether it is accurate), or where you have objected to the processing (and Educare11plus is considering whether its legitimate grounds override your interests)
- In limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format
- To withdraw consent to processing at any time (if applicable)
- To request a copy of an agreement under which personal data is transferred outside of the EEA.
- To object to decisions based solely on automated processing, including profiling
- To be notified of a data breach which is likely to result in high risk to their rights and obligations
- To make a complaint to the ICO or a Court.

Individual Responsibilities

During their employment, staff may have access to the personal information of other members of staff, suppliers, clients or the public. Educare11plus expects staff to help meet its data protection obligations to those individuals.
If you have access to personal information, you must:

- only access the personal information that you have authority to access and only for authorised purposes

- only allow other staff to access personal information if they have appropriate authorisation
- only allow individuals who are not Educare11plus staff to access personal information if you have specific authority to do so
- keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with the Educare11plus's policies).
- not remove personal information, or devices containing personal information (or which can be used to access it) from the Educare11plus's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device
- not store personal information on local drives or on personal devices that are used for work purposes.

Information Security

Educare11plus will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

All staff are responsible for keeping information secure in accordance with the legislation and must follow Educare11plus's acceptable usage policy.

Educare11plus will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Staff must maintain data security by protecting the confidentiality of the personal data. This means that only people who have a need to know and are authorised to use the personal data can access it.

Staff must maintain data security by protecting the integrity of the personal data. This means that personal data is accurate and suitable for the purpose for which it is processed.
Staff must maintain data security by protecting the availability of the personal data. This means that authorised users can access the personal data when they need it for authorised purposes.

Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards Educare11plus has implemented and maintains in accordance with the GDPR and DPA.
Where Educare11plus uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide that:

- the organisation may only act on the written instructions of Educare11plus
- those processing data are subject to the duty of confidence
- appropriate measures are taken to ensure the security of processing
- sub-contractors are only engaged with the prior consent of Educare11plus and under a written contract
- the organisation will assist Educare11plus in providing subject access and allowing individuals to exercise their rights in relation to data protection
- the organisation will delete or return all personal information to Educare11plus as requested at the end of the contract
- the organisation will submit to audits and inspections, provide Educare11plus with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell Educare11plus immediately if it does something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from the Data Protection Officer.

Storage and retention of personal information

Personal data will be kept securely in accordance with the Educare11plus's data protection obligations. Personal data should not be retained for any longer than necessary. The length of time data should be retained will depend upon the circumstances, including the reasons why personal data was obtained. Personal information that is no longer required will be deleted in accordance with Educare11plus's Record Retention Schedule.

Data breaches

A data breach may take many different forms:

- Loss or theft of data or equipment on which personal information is stored
- Unauthorised access to or use of personal information either by a member of staff or third party
- Loss of data resulting from an equipment or systems (including hardware or software) failure
- Human error, such as accidental deletion or alteration of data
- Unforeseen circumstances, such as a fire or flood
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams
- Blagging offences where information is obtained by deceiving the organisation which holds it

Educare11plus must report a data breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals. Educare11plus must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

Staff should ensure they inform their line manager or Data Protection Officer immediately that a data breach is discovered and make all reasonable efforts to recover the information, following Educare11plus's agreed breach reporting process.

Training

Educare11plus will ensure that staff are adequately trained regarding their data protection responsibilities.

Consequences of a failure to comply

Educare11plus takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and Educare11plus and may in some circumstances amount to a criminal offence by the individual.
Any failure to comply with any part of this policy may lead to disciplinary action under Educare11plus's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about this policy, you should contact your line manager or the Educare11plus's Data Protection Officer.

Review of Policy

This policy will be updated as necessary to reflect best practice or amendments made to the GDPR or DPA. This version was last updated on 28 February 2022.