Camphill School Aberdeen

Camphill Rudolf Steiner Schools Ltd, trading as Camphill School Aberdeen (CSA)

Data Protection Policy

Introduction

In this policy we set out the principles and procedures through which CSA secures its compliance with the General Data Protection Regulation (GDPR) enforced in the UK from 25th May 2018. For the purposes of the GDPR, CSA is the data controller and we determine the purposes and means of the processing of personal data described in this policy.

Policy Statement

In order to operate effectively CSA has to process personal information about people with whom it works. These may include current, past and perspective employees, volunteers, co-workers, trustees, clients, pupils, young adults and suppliers. In addition, it is required by law to process information to comply with government legislation.

CSA is committed to ensuring compliance with data protection legislation. CSA regards the lawful and correct treatment of personal information as essential to its successful operation and to maintaining confidence between CSA and all employees, volunteers, co-workers, trustees, clients, pupils, young adults and suppliers CSA will make every effort to ensure that data subjects can exercise their rights. Any breach of data protection legislation will be dealt with as a matter of urgency under CSA normal policies and procedures. If required breaches will be reported to the relevant authorities.

Data protection Principles

All processing of personal data must be conducted in accordance with data protection principles. The CSA policies and procedures are designed to ensure compliance with these principles.

1. Processing must be lawful and fair: processed lawfully, fairly and in a transparent manner in relation to the data subject.
2. Processing must be specified, explicit and legitimate: collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (‘purpose limitation’).
3. Personal data must be adequate, relevant and not excessive: adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’).
4. Personal data must be accurate and kept up to date: accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’).
5. Personal data must be kept for no longer than is necessary: kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (‘storage limitation’).

6. Personal data must be processed in a secure manner: processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

What is personal data?

1. All information about a person subject to automatic processing.
2. All information about a person contained (or intended to be contained) in a filing system relating to individuals, so as to permit easy access to the data, even if that system is dispersed on a functional or geographical basis.
3. Information is about a person if it concerns an identified or identifiable person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or factors specific to his physical, physiological, mental, economic, cultural or social identity. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used to identify the person.
4. Information about a person includes sounds and images.
5. The information can be factual or it can be an opinion about that person, their actions or behaviour.

What data is not covered?

1. Processing carried out by a person in the exercise of activities which are exclusively personal or domestic.
2. Data rendered anonymous in such a way that the individual is no longer identifiable.
3. Data kept in unstructured files.

What is meant by processing?

1. Collecting, capturing, recording, organising and storing data.
2. Adapting, manipulating or altering data.
3. Retrieving, consulting or using data.
4. Transmitting data.
5. Disclosing, communicating or otherwise making data available.
6. Erasing or destroying data.
7. Processing need not take place in the UK – GDPR applies wherever the processing takes place whether in the UK, Europe or otherwise.

Special Types of Data

This is particularly personal information including information about a person's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health and sexual orientation. The processing of such data is prohibited unless certain exceptional conditions apply, as it does when the data controller is engaged in the provision of social care.

Article 9 (h) of the GDPR allows the data controller to process special category data without consent in order to provide social care services. Unless one of the other exceptional conditions apply we will only process such information if it is essential to provide a person with the social care services they expect from us.

The other exceptional conditions under GDPR are as follows:

1. The data subject has given explicit consent to the processing of those personal data for one or more specified purpose.

2. It is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment provided, when the processing is carried out, the controller has an appropriate policy document in place.

3. It is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

4. It 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 and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.

5. It relates to personal data which are manifestly made public by the data subject.

6. It is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

7. It is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, preventive or occupational medicine, the provision of health care or treatment, the provision of social care, or the management of health care systems or services or social care systems or services, by or under the responsibility of a professional subject to the obligation of professional secrecy.

Professional Duty of Confidentiality

All those involved in providing education and social care are either registered with the appropriate professional body or under the direct supervision of someone who is. This means they have a professional obligation to treat personal data with the utmost confidentiality. In the case of social care this obligation is enforced by the Scottish Social Services Council (SSSC) and in the case of education services by the General Teaching Council for Scotland (GTCS).

Consent

It is our legal responsibility to provide high quality social care. To do so, it is vital to appreciate each individual's needs, preferences and interests so we can tailor our services appropriately. If we wish to use a person's data for purposes other than the provision of social care we must seek their explicit consent to do so. For example, if we wish to use personal stories or photographs for marketing or publicity purposes. We must explain to this to service users in the form of a written privacy notice. The privacy notice will explain what data we hold, why we hold it and the person's rights in relation to their data.

When processing personal data, it is important to be clear over the lawful grounds that we intend to use. There are six lawful grounds for processing and these are covered in the next section.

Where we rely on consent for the processing of personal data we should keep evidence of this. The request for consent should be separate from other matters and not hidden in the context of a written document, like a contract, that also concerns other matters.

Finally, the GDPR gives a specific right to withdraw consent. This means we will tell people about their right to withdraw, and offer them easy ways to withdraw consent at any time without penalty. Again, this will be done through the provision of a privacy notice that will also tell the person about their other rights in relation to their personal data. The law allows us to process the data without consent but only if an appropriate legal basis is established. In our case this is our legal duty to provide social care under the appropriate legal and regulatory framework.

Lawful Processing Requirements

As stated above, there are six lawful grounds for processing. The grounds must be determined before we begin processing, and this should be documented. Data processing must be done only if necessary and, if we can reasonably achieve the same purpose without the processing, we will not carry it out.

When processing special category or criminal information data we will identify both a lawful basis for general processing and an additional condition for processing this type of data. If a person is applying to work or volunteer with children or young people (under 18 years) and/or vulnerable adults, we are legally required to make background checks. A disclosure check is likely to be needed as a minimum, but the individual may also have to join the PVG Scheme run by Disclosure Scotland.

Processing is lawful only if and to the extent that at least one of the following applies:

1. The data subject has given consent to the processing of his or her personal data for one or more specific purposes.

2. 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.

3. Processing is necessary for compliance with a legal obligation to which the controller is subject.

4. Processing is necessary in order to protect the vital interests of the data subject or of another natural person.

5. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

6. Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Legitimate Interests Assessment

Where we need to rely on grounds other than consent in order to process personal data, we may choose to assert the *'legitimate interests'* of the organisation. To hold information in this way effectively restricts the individual's control over it so therefore we must complete a Legitimate Interest Assessment (LIA) for each category of personal data we want to hold under this lawful basis. This assessment shows that we have *weighed the balance of interests* between our own and the data subject and conclude in favour of our own.

Privacy Impact Assessment (PIA)

When introducing new technologies which involve processing likely to result in a high risk to the rights and freedoms of individuals, CSA will carry out a Data Protection Impact Assessment (DPIA).

Processing that is likely to result in a high risk includes systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals; large scale processing of special categories of data or personal data relating to criminal convictions or offences and large scale, systematic monitoring of public areas (CCTV). Other high-risk processing activities might include processing data concerning vulnerable data subjects, innovative use of technology or when the processing might prevent data subjects from exercising a right or using a service or a contract.

CSA will seek the views of data subjects or their representatives where appropriate in carrying out any DPIA which will consider the following: a) a description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller. b) an assessment of the necessity and proportionality of the processing in relation to the purpose. c) an assessment of the risks to individuals. d) The measures in place to address risk, including security and to demonstrate compliance with GDPR.

Data Subjects Rights

Data subjects have the following rights regarding data processing, and the data that is recorded about them:

1. To make subject access requests regarding the nature of information held and to whom it has been disclosed
2. to have your personal data corrected where it is inaccurate;
3. to have your personal data erased where it is no longer required. Provided that we do not have any continuing lawful reason to continue processing your personal data, we will make reasonable efforts to comply with your request;
4. that your personal data be transferred to another person;
5. to restrict the processing of your personal data where you believe it is unlawful for us to do so, you have objected to its use and our investigation is pending, or you require us to keep it in connection with legal proceedings; and
6. to object to the processing of personal data, where CSA rely on **legitimate business** interests as a lawful reason for the processing of personal data. individuals also have the right to object where we are processing your personal information for direct marketing purposes. Except for the purposes for which we are sure we can continue to process your personal data, we will temporarily stop processing your personal data in line with your objection until we have investigated the matter. If we agree that your objection is justified in accordance with your rights, we will permanently stop using your data for those purposes. Otherwise, we will provide you with our justification as to why we need to continue using your data.

Subject Access Requests

Individuals have a right to see the personal data CSA hold in relation to them. This is not a new right but was already enshrined under the Data Protection Act. The individual also has the right to challenge all the personal data held about them. There is very little exemption for this – it is only possible to refuse to let the subject see the data in the very limited scenario where the data relates to certain forms of business planning (such as redundancy plans). We cannot refuse the subject access to their personal data simply because it is contrary to our business interests. The remainder of this section sets out how we will manage and respond to a subject access request.

Confirm the identity of the person making the request.

Individuals are generally only entitled to information about themselves. If we are being asked to supply information to an email or postal address, does that conform to the address we have on record for that individual? If not we may wish to ask for proof of identity. We must take reasonable steps to ensure that the request is genuinely from the individual concerned.

If the person making the request is acting on behalf of another we should ask for evidence of their authority, for example a consent form.

First Response

A letter will be sent by email confirming our receipt of their request and giving an indication of when they might expect to receive a full response.

If CSA decide to refuse their request we will respond within one month explaining our grounds for not complying and informing them of their right to complain to the ICO (information commissioner's office) and/or to seek a legal remedy.

Preparing a response

The right of access allows individuals to be aware of and verify the lawfulness of the processing. To enable an individual to do that they are also entitled to know:

- the purposes of the processing
- the categories of data processed
- the recipients or categories of recipient to whom the data has been or will be disclosed
- the envisaged period for which the data will be stored, or, if not possible, the criteria used to determine that period
- the source of the data where the personal data was not collected from the individual
- the existence of automated decision making
- if the data is sent out of the EU, to be told what appropriate safeguards are in place

Third party data

Data about an individual might incidentally contain reference to a third party. Information from which a third party could be identified should be redacted (blanked out). Where that occurs, it should be explained to the individual that some information has been withheld, and why. Alternatively, or if the third party could still be identified after redaction, we should seek the consent of that third party before disclosing the data.

Exemptions

We are not obliged to disclose information to an individual to the extent that doing so would involve disclosing information relating to another individual who can be identified from the information unless the other individual has consented to the disclosure or it is reasonable to disclose the information to the individual without consent.

We are not obliged to disclose information in respect of which a claim to confidentiality of communications could be maintained in legal proceedings. Confidentiality of communications is (in Scotland) a right of absolute privilege in respect of communications between a solicitor or advocate and a client relating to advice and also in respect of any documents which were prepared in the contemplation of litigation whether involving a solicitor or not such as expert reports and witness statements.

We are not obliged to disclose data processed for the purposes of management forecasting or management planning in relation to a business or other activity, to the extent that disclosure would be likely to prejudice the conduct of the business or activity concerned.

We are not obliged to disclose data that consists of records of our intentions in relation to any negotiations with the individual to the extent that disclosure would be likely to prejudice those negotiations.

We are not obliged to disclose references given by us in confidence about an individual for the purposes of education, training, employment, appointment to any office, or the provision of any service by the individual (but that does not apply to references given to us).

We must not disclose data concerning health that is not already known by the data subject unless we have an opinion from the appropriate health professional that the serious harm test is not met. The serious harm test is: disclosure would be likely to cause serious harm to the physical or mental health of the individual or another individual.

Other exemptions may apply including data relating to national security, the prevention or detection of crime, the apprehension or prosecution of offenders, the assessment or collection of a tax, the maintenance of immigration control, compliance with an enactment or order of court, information used for journalistic, academic, artistic or literary purposes, the discharge of certain functions of a public nature exercised in the public interest such as health and safety or maladministration and data used for research and statistics.

The Response

Normally our response will be to provide the data requested. We should ensure everything that is being provided in response to a SAR is itemised in a covering letter. We should explain the format in which we are providing the data and why it was chosen. An individual may have asked for the information in a particular format e.g. a hard copy. Otherwise, if the request was in electronic form we must provide them with the information in electronic form.

Where we have decided not to provide some or all of the data requested, we must explain why and inform the individual that if they are unhappy with this decision they have a right to complain to the ICO (information commissioner's office) and/or to seek a judicial remedy.

If the information is redacted we must explain that and give the reason for the redaction. For example: 'some names and identifying particulars have been deleted to protect the identity of third parties'.

Individual Rights over their Personal Data

The individual has the right of rectification, erasure, restriction and objection. These are described below.

<u>Rectification</u>

An individual has a right to obtain the rectification of incorrect personal data or to have incomplete data completed, for example by the provision of a supplementary statement. On receipt of a request for rectification steps should be taken to rectify the data without unreasonable delay. We are also obliged to inform all third parties to whom we have disclosed the information of the rectification (unless this is impossible or involves disproportionate effort) and let the individual know who those recipients are if requested.

<u>Erasure</u>

Individuals have the right to request the erasure of the personal data that we hold about them, also known as the right to be forgotten, in certain circumstances. These include:

- The data is no longer necessary for the purpose we collected it for.
- The individual has withdrawn their consent to us processing it and no other legal justification for processing applies.
- The individual objects to processing for direct marketing purposes.
- We are unlawfully processing their data.

Once an individual requests erasure for one of the above reasons, we must erase it without delay unless continued retention is necessary for other legitimate purposes including:

- Exercising the right of freedom of expression and information.
- Complying with a legal (statutory) obligation.
- The performance of a task carried out in the public interest.
- The establishment, exercise, or defence of legal claims.

If erasure is appropriate and we have made the data public, we must also take reasonable steps, including technical measures, to inform other data controllers that are processing the personal data about the individual's erasure request. This includes removing any links to the personal data as well as any copies of the personal data.

Restriction

Individuals have the right to restrict the processing of their personal data under certain circumstances. These include:

- The individual contests the accuracy of the personal data. If so we must restrict processing the contested data until we can verify its accuracy.
- The processing is unlawful. Instead of requesting erasure, the individual can request that we restrict use of the unlawfully processed personal data.
- We no longer need to process the personal data but the individual needs the personal data for the establishment, exercise, or defence of legal claims.
- The individual objects to processing that relies on the public interest or our or a third party's legitimate interests as the lawful processing ground. We are required to restrict the challenged processing activity pending verification of whether our or a third party's legitimate interests override the individual's interests.

When an individual request a data processing restriction, we can continue to store the personal data, but may only process it in certain circumstances including:

- With the data subject's consent.
- To establish, exercise, or defend legal claims.

- To protect the rights of another individual or legal entity.
- For important public interest reasons.

Before lifting the data processing restriction, we must notify the individual.

Objection

Individuals have the right to object to data processing under certain circumstances, including:

- For direct marketing purposes, including profiling related to direct marketing. We must stop processing a data subject's personal data for direct marketing purposes when the person objects.
- For scientific or historical research purposes or statistical purposes unless the processing is necessary for the performance of a task carried out in the public interest
- For processing, including any profiling, based on necessity to perform a task in the public interest or necessity for our or a third party's legitimate interests. If the individual objects to processing in these circumstances, we must stop processing the personal data unless we can demonstrate a compelling legitimate ground for processing the personal data that overrides the individual's interests or needs to process the personal data to establish, exercise, or defend legal claims.

Data Breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. Under the Data Protection Act there was no obligation to report data breaches. However, the GDPR introduces a data breach notification requirement and potentially high penalties for non-compliance.

When a personal data breach has occurred, we need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then we must notify the ICO; if it's unlikely then we don't have to report it. However, if we decide we don't need to report the breach, we need to be able to justify this decision, so we should document it.

If the breach results in a risk to an individual's freedoms and rights, and if there is a high risk, we must in addition report the breach to the data subjects themselves.

If we use a data processor, and this processor suffers a breach, then it must inform us without undue delay. We in turn notify the ICO.

Within 72 hours of a reportable breach the data controller must notify the ICO of:

1. the nature of the data breach (including the categories of data, number of data records and number of data subjects affected)
2. the name and contact details of any data protection officer or other contact

3. the likely consequences of the breach
4. the measures taken or intended to be taken to address the breach
5. the measures taken to mitigate any possible adverse effects.

We must maintain documentation on data breaches, their nature and what remedial actions we took.

Data Transfers

CSA to not envisage any data processing scenario that would involve data transfer to out with the European Economic Area (EEA). This will be only be undertaken where the data subject has explicitly consented to any proposed transfer, or the transfer is necessary by law, for public interest or to protect the vital interests of the data subject where the data subject is physically, mentally or legally incapable of giving consent.

Data Security

CSA will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including where appropriate:

- The pseudonymisation and encryption of personal data
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems.
- The ability to restore the availability and access to personal data in a timely manner in the event of any physical or technical incident.

Retention and Disposal of Data

CSA will keep personal data and special category personal data for as long as is necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Some information may be held for a long period of time as part of a safeguarding risk management programme.

The retention period varies depending on the category of personal data we hold. At the expiry of the set retention period, or in other select circumstances, your personal data will be permanently and securely deleted.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use and retain such information without further notice to you, as it falls outside of the definition of personal data under the GDPR.

All personal data will be securely disposed of.

Training

CSA will ensure that all personnel and processors who have access to CSA personal data receive the appropriate training, in order to comply with data protection legislation. CSA Managers are responsible for assuring appropriate training has been undertaken, including for temporary or contracted staff.

Outcomes and Impacts

- To prevent the inappropriate use of data held by CSA.
- Ensure CSA personnel are aware of their responsibilities for handling personal data and that failure to do so could result in disciplinary proceedings.
- Training requirements are identified and staff/ volunteers have the required level of data protection knowledge.
- Uphold data subject rights
- Ensure CSA compliance with data protection legislation

CSA Data Protection Officer

If you require any further information about how we use your personal data, or wish to raise a concern you should contact: CSA data protection officer Central Office, Murtle Estate, Bieldside, Aberdeen, AB15 9EP Tel 01224 866158 email office@crss.org.uk

The Information Commissioners Office (ICO)

The ICO is the UK's independent body set up to uphold information rights. If you have concerns that we cannot resolve or wish to contact them for any other reason you can phone them on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire.

Related Policies / Documents

Data protection Privacy Notices

a) Employees, Co-workers, Volunteers and Trustees
b) Service Users/ Pupils/ Young Adults / Parents and Guardians
c) Suppliers

ICT Security Policy
Safeguarding Policy
Records Management Policy

Record of Approval				
1	*May 2018*	*Kathleen Scott*	*(For Executive Team)*	*(for Board of Trustees)*
Rev	***Date***	***Author***	***Recommended***	***Approved***