Camphill Wakefield

Data Protection Policy

Approved by:	Board of Trustees	**Date:** 17th October 2024
Last reviewed:	September 2026	
Next review due:	September 2027	

Document Control			
Policy Owner		**Executive Director: Quality, Performance and People**	
Version	**Author**	**Date**	**Changes/Updates**
V0.1	Bethan Artro Morris	10.07.24	Draft policy written
V1	Bethan Artro Morris		**Approved by the Board – 17.10.24**
V2		19.02.25	P5 – Data Protection Principles – Pseudonymisation added
		September 2025	Reviewed by CEO – no changes/updates
V2.1		August 2026	Annual review completed. Updated to reflect the Executive Director leadership structure and changes to UK data protection legislation introduced by the Data (Use and Access) Act 2025, including subject access requests, data protection complaints, automated decision-making and international data transfers.
V3	Helen Kain	30.09.26	Role and DPO details updated;

Introduction and Scope

Camphill Wakefield is required to process personal information about staff, students, parents, guardians, and other individuals we may interact with. We must do this in compliance with data protection and other relevant legislation.

This policy provides a framework for ensuring that we comply with the requirements of the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 (DPA), as amended by the Data (Use and Access) Act 2025, Environmental Information Regulations 2004 (EIR) and Freedom of Information Act 2000 (FOIA), together with associated statutory guidance and Codes of Practice.

Prompt, honest reporting of errors and near misses is encouraged. An accidental breach does not automatically amount to misconduct; any disciplinary response must follow a fair assessment of the circumstances under the Disciplinary Policy.

This policy, including its appendices, applies to our entire workforce. This includes employees, Trustees, contractors, agents and representatives, volunteers and temporary staff working for, or on behalf of, the organisation. Individuals who are found to knowingly or recklessly infringe this policy may face disciplinary action.

This policy is the organisation's main information governance policy and applies to all personal data, regardless of whether it is in paper or electronic format.

The policy covers the College, Day Services and enterprise activities, including the café, and personal data about students, graduates, service users, staff and other individuals. It applies to the systems, records and evidence we use or share across these activities.

Information security, data breaches, acceptable use of systems and records management are addressed in separate policies.

All actual or suspected personal data breaches must be reported immediately to the Executive Director and DPO using the Data Breach Policy. Do not delay an initial alert while completing a form. Record every breach, including those not notified externally, and preserve evidence. The statutory notification decision is made by the accountable lead with DPO advice.

Roles and Responsibilities

Overall responsibility for ensuring that the organisation meets the statutory requirements of any data protection legislation lies with the Trustees. The following roles have day to day responsibility for compliance and provide the necessary assurance to the Board.

Data Protection Officer (DPO)

Judicium Consulting Limited provides Camphill Wakefield's independent DPO service, advising on UK GDPR and Data Protection Act 2018 obligations and monitoring compliance. Camphill Wakefield remains accountable as the data controller. The DPO must be involved promptly in relevant decisions and incidents.

Data Protection Officer: Judicium Consulting Limited
Email: dataservices@judicium.com
Website: www.judiciumeducation.co.uk
Published address: 98 Theobalds Road, London, WC1X 8WB
Published telephone: 0345 548 7000 option 1

ACTION BEFORE APPROVAL: Confirm the contracted Judicium contact details and urgent breach reporting route. Update the Data Breach Policy, privacy notices and linked documents to use the same confirmed details.

Schools Data Protection Officer
Veritau
West Offices
Station Rise
York
North Yorkshire
YO1 6GA

schoolsDPO@veritau.co.uk // 01904 554025

The DPO is an advisory role, and its duties include:

- Informing and advising us and our employees about our obligations to comply with UK GDPR and other data protection laws,
- Monitoring compliance with data protection legislation and internal policies,
- Raising awareness of data protection issues and conducting compliance reviews, and
- Liaising with the Information Commissioners Office (ICO).

Senior Information Risk Owner (SIRO)
The SIRO is a senior leader with responsibility for oversight of information risk, ensuring that the organisation's policies and procedures are effective, comply with legislation and promote good information governance practice.

At Camphill Wakefield, the SIRO role will be held by a nominated Executive Director.

A DPIA will be considered before introducing new technologies or systems involving personal data, including Artificial Intelligence (AI), automated decision-making, biometric technologies or other processing likely to result in a high risk to individuals' rights and freedoms.

Automated Decision-Making and Artificial Intelligence

Where Camphill Wakefield uses automated processing or Artificial Intelligence involving personal data, it will ensure that an appropriate lawful basis has been identified and that the processing complies with data protection by design and default.

Where solely automated processing is used to make a significant decision about an individual, appropriate safeguards will be applied in accordance with data protection legislation. These will include providing appropriate information about the decision and enabling the individual to make representations, obtain meaningful human intervention and contest the decision where required.

Special category data will only be used in automated decision-making where the additional statutory requirements are satisfied.

Staff must not enter confidential, sensitive or identifiable student, staff or organisational information into publicly available AI systems unless the use has been expressly authorised and appropriate data protection controls are in place.

Single Point of Contact (SPOC)
The SPOC is someone who can take operational responsibility for data protection, including communicating with data subjects and the DPO. At Camphill Wakefield, this role lies with the Governance and Policy Officer

Information Asset Owner
An IAO is an individual who is responsible for the security and maintenance of a particular information asset. They are responsible for ensuring that other members of staff are using the information safely and responsibly. We will ensure that IAO's are appointed based on sufficient seniority and level of responsibility, and document this in our Information Asset Register (IAR).

All Staff
All staff, including trustees, contractors, agents and representatives, volunteers and temporary staff working for, or on behalf of, the organisation are responsible for collecting, storing and processing any personal data in accordance with this policy.

Data Protection Principles

We will comply with the data protection principles, as defined in Article 5 of the UK GDPR. We will ensure that personal information is:

- Processed lawfully, fairly and in a transparent manner **(Lawfulness, Fairness and Transparency).**
- Collected only for specified, explicit and legitimate purposes **(Purpose Limitation).**
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed **(Data Minimisation).**
- Accurate and where necessary kept up to date **(Accuracy).**
- Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed **(Storage Limitation).**

- Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or **damage (Security, Integrity and Confidentiality).**
- Protected by the process of Pseudonymisation whereby personally identifiable information fields within a data record are replaced **(Pseudonymisation)**

We recognise that not only must we comply with the above principles, we must also demonstrate our compliance **(Accountability).**

Lawful Bases

UK GDPR sets out several conditions under which we can process personal information lawfully. We usually rely on the lawful basis of Public Task or Legal Obligation, however at times we may rely on our legitimate interests. We will only do this where we are using data in ways individuals would reasonably expect and will carry out an appropriate legitimate interest assessment (LIA) prior to starting the processing.

We have an Appropriate Policy Document (APD) in place (see Appendix One) which provides information about our processing of special category (SC) and criminal offence (CO) data. The APD demonstrates how we comply with the requirements of the UK GDPR and DPA.

Consent

We generally only obtain consent where there is no other lawful basis, for example when taking photographs or videos intended for publication. We will ensure that consent is clear and transparent and can be withdrawn at any time, in accordance with the UK GDPR. We will regularly review consents to check that the relationship, the processing, and the purposes have not changed.

Where appropriate, we will seek consent directly from students in line with the Mental Capacity Act (2005). Where this is not appropriate, we will seek consent from the parent or carer.

Data Subject Rights

Under the UK GDPR, individuals have several rights in relation to the processing of their personal data:

Right to be informed

We provide individuals with privacy information at the time we collect their data, normally by means of a privacy notice, which is made easily accessible to the data subject. Privacy notices will be clear and transparent, regularly reviewed, and include all information required by data protection legislation.

Right of access

Individuals have the right to access and receive a copy of the information we hold about them. This is commonly known as a subject access request (SAR). We have in place a SAR procedure which details how we deal with these requests (Appendix Two).

Other rights include the right to rectification, right to erasure, right to restrict processing, right to object, right to data portability and rights related to automated decision-making, including profiling.

Requests exercising these rights can be made to any member of staff, but we encourage requests to be made in writing, wherever possible, and forwarded to the Communications and Marketing Manager (SPOC), who will acknowledge the request and respond within one calendar month. Advice regarding such requests will be sought from our DPO where necessary.

A record of decisions made in respect of the request will be retained, recording details of the request, whether any information has been changed, and the reasoning for the decision made.

Records of Processing

In accordance with Article 30 of UK GDPR, we must keep a record of our processing activities. We will do this by developing and maintaining an Information Asset Register (IAR) which will include as a minimum:

- The organisation's name and contact details,
- The name of the information asset,
- The owner of that asset, known as the Information Asset Owner (IAO),
- The purposes of the processing,
- A description of the categories of individuals and the types of personal data,
- Who has access to the personal data, and who it is shared with,
- The lawful bases for each processing activity,
- The format and location of the personal data,
- Details of any transfers to third countries, and the appropriate safeguards,
- The retention periods for each asset,
- A general description of the technical and organisational security measures.

We will include links to relevant documentation, such as data processing contracts, information sharing agreements, and risk assessments, wherever possible.

We will review the IAR at least annually to ensure it remains accurate and up to date, consulting with the DPO as necessary.

Privacy by Design and Risk Assessments

We will adopt a privacy by design approach and implement appropriate technical and organisational security measures to demonstrate how we integrate data protection into our processing activities.

We will conduct a data protection impact assessment (DPIA) when undertaking new, high-risk processing, or making significant changes to existing data processing. The purpose of the DPIA is to consider and document the risks associated with a project prior to its implementation, ensuring data protection is embedded by design and default.

All of the data protection principles will be assessed to identify specific risks. These risks will be evaluated and solutions to mitigate or eliminate these risks will be considered. Where a less privacy-intrusive alternative is available, or the project can go ahead without the use of special category data, we will opt to do this.

All DPIAs are signed by our Senior Information Risk Owner and Data Protection Officer.

Information Sharing

In order to efficiently fulfil our duty of education provision it is sometimes necessary for us to share information with third parties. Routine and regular information sharing arrangements will be documented in our privacy notices and in our IAR.

Any further or ad-hoc sharing of information will only be done so in compliance with legislative requirements, including the ICO's data sharing code of practice. We will only share personal information where we have a lawful basis to do so, ensuring any disclosure is necessary and proportionate. All disclosures will be approved by the relevant staff member and recorded in a disclosure log.

Contract Management

All third-party contractors who process data on our behalf must be able to provide assurances that they have adequate data protection controls in place. Where personal data is being processed, we will ensure that there is a written contract in place which includes all the mandatory data processing clauses, as required by UK GDPR.

We will maintain a record of our data processors, and regularly review the data processing contracts, with support from the DPO, to ensure continued compliance.

International Transfers

Where personal data is transferred outside the UK, Camphill Wakefield will ensure that the transfer complies with the requirements of UK data protection legislation.

This may include reliance on UK adequacy regulations or the implementation of appropriate safeguards, such as an approved International Data Transfer Agreement or UK Addendum, together with any required transfer risk assessment.

We will consult our DPO before entering into arrangements involving restricted international transfers where appropriate.

Training

We will ensure that appropriate guidance and training is given to our workforce, governors or Trustees, and other authorised persons on data protection and access to information. Training will be delivered as part of the induction process and as refresher training at appropriate intervals.

Specialised roles or functions with key data protection responsibilities, such as the SIRO, SPOC and IAOs, will also receive additional training specific to their role.

We will keep a record of all training that has been completed and ensure that data protection awareness is raised in staff briefings and as standard agenda items in meetings, where appropriate.

Complaints

Anyone may raise a data protection complaint with the SPOC, Executive Director or DPO. Staff who receive a complaint must forward it promptly. Provide an accessible route; acknowledge receipt within 30 days, make appropriate enquiries, keep the complainant informed and communicate the outcome without undue delay. A complaint indicating a possible breach must also be assessed immediately under the Data Breach Policy.If an individual remains dissatisfied after we have concluded our investigation, they may complain to the Information Commissioner's Office. Their contact details are below:

Phone: 0303 123 1113 or via their live chat. Their normal opening hours are Monday to Friday between 9am and 5pm (excluding bank holidays). You can also report, enquire, register and raise complaints with the ICO using their web form on Contact us | ICO.

Policy Review

This policy will be reviewed annually by the Executive Directors, in consultation with the Data Protection Officer where appropriate. It will also be reviewed sooner where there are significant changes to legislation, regulatory guidance or Camphill Wakefield's information governance arrangements. Where there are significant changes approval by the Board of Trustees is needed.

Appendix One – Appropriate Policy Document

Introduction

Camphill Wakefield processes special category and criminal conviction data in the course of fulfilling its functions as a college and social care provision. Schedule 1 of the Data Protection Act 2018 requires data controllers to have in place an 'appropriate policy document' where certain processing conditions apply for the processing of special categories of personal data and criminal convictions data. This policy fulfils this requirement.

This policy complements our existing records of processing as required by Article 30 of UK General Data Protection Regulation, which has been fulfilled by the creation and maintenance of an Information Asset Register. It also reinforces our existing retention and security policies, procedures and other documentation in relation to special category data.

Special Categories and Conditions of Processing

We process the following special categories (SC) of data:

- racial or ethnic origin,
- religious or philosophical beliefs,
- trade union membership,
- health,
- sex life/orientation,

We also process criminal offence (CO) data under Article 10 of UK GDPR, including for pre-employment checks and declarations by employees in line with their contractual obligations.

We rely on the following processing conditions under Article 9 of UK GDPR and Schedule 1 of the Data Protection Act 2018 to lawfully process special category and criminal convictions data:

For every activity we identify an Article 6 lawful basis. Special category data also requires an Article 9 condition and, where that condition requires it, a DPA 2018 Schedule 1 condition. Criminal offence data is governed separately by Article 10 and requires official authority or an applicable Schedule 1 condition under domestic law.
Article 9(2)(a) – explicit consent
Explicit consent must be freely given, specific, informed and confirmed in a clear oral or written statement identifying the special category data and purpose. An implied affirmative action alone is insufficient. Record the statement, make withdrawal easy and regularly review the consent.

Examples of such processing includes when we ask for health or medical information from visitors to aid them in the event of an emergency.

Article 9(2)(b) – employment, social security or social protection
To comply with our legal requirements as an employer and safeguard our students, we need to collect some special category data.

Examples include processing staff health information for reasonable adjustments and absence management, and relevant trade union information where necessary for employment obligations. DBS checks involve criminal offence data and must be assessed separately under Article 10 and the appropriate Schedule 1 condition.

Examples include when we carry out DBS checks on staff to evidence suitability for a role; collect medical information to put in reasonable adjustments at work and monitor staff absence; and keep records of an employee's trade union membership.

When processing information under Article 9(2)(b), we also require a Schedule 1 condition under the Data Protection Act 2018. The condition we rely on for this processing is **Schedule 1, Part 1, (1) - employment, social security and social protection.**

Article 9(2)(g) – reasons of substantial public interest
We have a wide variety of duties we must carry out in the public interest. Much of our processing of SC data is done so for the purposes of substantial public interest.

Examples include when we process SC data to identify students who require additional support such as special educational needs; processing safeguarding concerns to ensure the safety and wellbeing of students; or collecting medical information when monitoring student attendance or dietary requirements.

When processing data under Article 9(2)(g), we also require a Schedule 1 condition under the Data Protection Act 2018. The conditions we rely on for this processing are **Schedule 1, Part 2, (6) – statutory and government purposes; (10) – preventing or detecting unlawful acts; and (18) – safeguarding of children and of individuals at risk.**

Compliance with Data Protection Principles

We have several policies and procedures in place to ensure our compliance with the Article 5 Data Protection Principles and meet our accountability obligations, explained in more detail below:

Accountability Principle
We have put in place appropriate technical and organisational security measures to meet the requirements of accountability. These include:

-
- The appointment of Judicium Consulting Limited as our independent DPO, with appropriate reporting and access to the Executive Director and Trustees.Taking a data protection by design and default approach to our processing activities, including the use of risk assessments.
- Maintaining documentation of our processing activities through an Information Asset Register.
- Adopting and implementing information governance policies and ensuring we have written contracts in place with data processors.
- Implementing appropriate security measures in relation to the personal data we process. More detail can be found in our Information Security Policy

Principle (a): lawfulness, fairness and transparency
Identify the Article 6 lawful basis for each purpose. Where special category data is processed, identify the Article 9 condition and any required Schedule 1 condition; where criminal offence data is processed, identify the Article 10 authority and domestic law condition. Keep the assessment in our processing records. We consider how any processing may affect individuals concerned and provide clear and transparent information about why we process personal data, including our lawful bases, in our privacy notices and this policy document. All privacy notices provide details of data subject rights. Our privacy information is regularly reviewed and updated to ensure it accurately reflects our processing.

Principle (b): purpose limitation
Schools and colleges can only act in ways and for purposes which they are empowered to do so by law. Personal data is therefore only processed to allow us to carry out the necessary functions and services we are required to provide in line with legislation. We clearly set out our purposes for processing in our privacy notices, policies and procedures, and in our IAR. If we plan to use personal data for a new purpose, other than a legal obligation or function set out in law, we check that it is compatible with our original purpose, or we obtain specific consent for the new purpose.

Principle (c): data minimisation
Use personal data only for specified lawful purposes documented in privacy notices and the IAR. Before reusing it for a different purpose, assess whether the new use is compatible or supported by an appropriate legal provision or valid consent. Document the decision and give updated privacy information where required.

Principle (d): accuracy
Take reasonable steps to correct inaccurate personal data without delay, considering the purpose for which it is held. Where an opinion or historical record is disputed, record the challenge and distinguish it from established facts. Consider restriction while accuracy is checked. Erasure and rectification are different rights; a lawful basis requiring retention does not by itself remove the duty to correct inaccuracies. Notify recipients of rectification as required and record decisions and any lawful exemption.

Principle (e): storage limitation
We have a Retention Schedule in place which is based on guidance issued by the Information and Records Management Society (IRMS). Where there is no legislative or best practice guidance in place, the SIRO will decide how long the information should be retained based on the necessity to keep the information for a legitimate purpose or purposes. We also maintain a Destruction Log, which documents what information has been destroyed, the date it was destroyed and why it has been destroyed. Further information can be found in our Records Management Policy.

Principle (f): integrity and confidentiality (security)
We employ various technical and organisational security measures to protect the personal and special category data that we process. A full description of security measures can be found in our Information Security Policy.

Report every actual or suspected personal data breach promptly to the Executive Director and DPO under the Data Breach Policy and record confirmed breaches and the response. Notify the ICO unless the breach is unlikely to result in a risk to individuals' rights and freedoms, without undue delay and where feasible within 72 hours of awareness. Notify affected individuals without undue delay where high risk is likely. Record reasons for notification or non-notification..

Retention of special category and criminal convictions data

The retention periods of special category and criminal convictions data are set out in our Retention Schedule. Retention periods of specific information assets are identified in our Information Asset Register and we have in place a Records Management Policy.

Keep this Appropriate Policy Document under review and retain it for at least six months after the relevant processing ends. Make it available to the ICO on request. The IAR and retention schedule must identify actual retention periods for the special category and criminal offence records concerned; record any departure and the reasons.

Appendix Two – Subject Access Request (SAR) Procedure

Under the UK GDPR, individuals have the right to make a subject access request (SAR) to any member of our workforce, or Trustee, or contractor or agent working for the organisation. Requests need not be made in writing, but we encourage applicants to do so where possible. Requests should be forwarded the Communications and Marketing Manager who will log the request and acknowledge it within five college days.

We must be satisfied of the requestor's identity and may have to ask for additional information to verify this, such as:

- valid photo ID, such as driver's licence or passport,
- proof of address, such as a utility bill or council tax letter, or
- confirmation of email address.

Only once we are confident of the requestor's identity and have sufficient information to understand the request will it be considered valid. We will then respond to the request within the statutory timescale of one calendar month.

We can apply a discretionary extension of up to a further two calendar months to comply if the requested information would take a considerable amount of time to respond, due to either the complexity or volume of the records. If we wish to apply an extension, we will firstly seek guidance from our DPO, then inform the applicant of the extension within the first calendar month of receiving the request.

If we think it necessary to apply any exemptions, we will seek guidance from our DPO. In limited circumstances, we may also refuse a request on the basis that it is manifestly unfounded or excessive

Requests received from parents asking for information falling under the student's education record will be dealt with under the Education (Pupil Information) (England) Regulations 2005 and responded to within 15 college days. Any charges which arise from this request will be applied at our discretion.

When responding to a Subject Access Request, Camphill Wakefield will undertake reasonable and proportionate searches for the personal information requested.

Where reasonably required to identify the information or processing activities to which a request relates, we may seek clarification from the requester. Where permitted by legislation, the statutory response period may be paused while clarification is awaited. The requester will be informed where this applies.

Data Protection Complaints

Camphill Wakefield will facilitate the making of complaints about its processing of personal data and will provide an accessible means by which individuals can raise a concern.

Complaints should normally be directed to the Single Point of Contact (SPOC), although a complaint received by another member of staff must be forwarded promptly.

We will:

- acknowledge a data protection complaint within 30 days;
- take appropriate steps to investigate the complaint;
- keep the complainant appropriately informed about progress;
- respond with the outcome without undue delay; and
- provide information about the individual's right to complain to the Information Commissioner's Office.

Advice will be sought from the DPO where appropriate.

If an individual remains dissatisfied after we have concluded our investigation, they may appeal to the Information Commissioner's Office. Their contact details are below:

Phone: 0303 123 1113 or via their live chat. Their normal opening hours are Monday to Friday between 9am and 5pm (excluding bank holidays). You can also report, enquire, register and raise complaints with the ICO using their web form on Contact us | ICO.

Camphill Wakefield

Appendix Three – Freedom of Information (FOI) and Environmental Information Regulation (EIR) Requests

Freedom of Information (FOI)
The Freedom of Information Act 2000 (FOIA) is part of the Government's commitment to greater openness and transparency in the public sector. It enables members of the public to scrutinise the decisions of public authorities more closely and ensure that services are delivered properly and efficiently. Schools and colleges have two main responsibilities under the Freedom of Information Act:

- To publish certain information about its activities in a publication scheme, and
- To process and respond to individual requests for information, with a duty to provide advice and assistance.

Under FOI, anyone can request access to general recorded information we hold. Recorded information includes printed documents, computer files, letters, emails, photographs, and sound or video recordings. A Code of Practice under section 45 of the Act sets out recommendations for the handling of requests for information. To comply with this Code requests must:

- Be in writing,
- Provide the name or company name and contact address or email address,
- Describe the information they are requesting,
- Ideally, state the preferred format they would like the information to be provided.

Any request that cannot be answered promptly as part of normal day to day business or where we are asked to handle it under Freedom of Information, will be treated as a FOI request.

Information can be withheld if one or more of the 24 exemptions within the FOIA apply. This could mean that certain information is not released in response to a request or is not published. Requests for information can be refused for reasons including:

- The information is not held
- It would cost too much or take too much staff time to comply with the request
- The request is considered vexatious
- The request repeats a previous request from the same person.

Environmental Information Regulations (EIR)
Requests for information that relates to the environment, including activities which may affect the environment, are dealt with under the Environmental Information Regulations 2004. EIR is similar to FOI but there is an even greater presumption of disclosure, and there are fewer exceptions under which a request can be refused. Requests under EIR can also be given verbally and do not need to be in writing, but must include:

- A name or company name and contact address or email address,
- A description of the information being requested,
- Ideally, the preferred format they would like the information to be provided.

“Environmental Information” includes information which relates to:

a. the state of the elements of the environment, such as air and atmosphere, water, soil, land, landscape and natural sites including wetlands, coastal and marine areas, biological diversity and its components, including genetically modified organisms, and the interaction among these elements,

b. factors such as substances, energy, noise, radiation or waste, including radioactive waste, emissions, discharges and other releases into the environment, affecting or likely to affect the elements of the environment referred to in (a),

c. measures (including administrative measures), such as policies, legislation, plans, programmes, environmental agreements, and activities affecting or likely to affect the elements and factors referred to in (a) and (b) as well as measures or activities designed to protect those elements,

d. reports on the implementation of environmental legislation,

e. cost-benefit and other economic analyses and assumptions used within the framework of the measures and activities referred to in (c), and

f. the state of human health and safety, including the contamination of the food chain, where relevant, conditions of human life, cultural sites and built structures in as much as they are, or may be affected by the state of the elements of the environment referred to in (a) or, through those elements, by any of the matters referred to in (b) and (c).

Requests for information under FOI and EIR
Any requests received should be forwarded to the Communications and Marketing Manager who will log the request and acknowledge within five college days.

The Communications and Marketing Manager is responsible for:

- Deciding whether the requested information is held,
- Locating, retrieving or extracting the information,
- Considering whether any exemption or exception might apply, and the balance of the public interest test,
- Preparing the material for disclosure and drafting the response,
- Seeking any necessary approval for the response, and
- Sending the response to the requester.

Requests for information under FOI and EIR
Forward requests immediately to the SPOC and Executive Director. Log receipt, the

applicable regime and response deadline. Acknowledge promptly and arrange cover during holidays or absence. Seeking internal approval must not delay a required response.

The delegated SPOC, supported by the Executive Director, is responsible for:

Deciding whether the requested information is held,

Locating, retrieving or extracting the information,

Considering whether any exemption or exception might apply, and the balance of the public interest test,

Preparing the material for disclosure and drafting the response,

Seeking any necessary approval for the response, and

Sending the response to the requester.

FOI requests must normally be in writing, give the requester's real name and a correspondence address, and describe the information requested. Provide reasonable advice and assistance and accessible support. Use safe IT procedures for electronic links rather than automatically rejecting a request. EIR requests may be verbal; record them and seek any clarification needed.

The Chair of Trustees and the Executive Director: Quality, Performance and People will jointly consider the public interest test and uncertain exemptions, with DPO or legal advice where appropriate and within the applicable deadline.

- Document clearly the benefits of both disclosing or withholding the requested information,
- Where necessary seek guidance from previous case law in deciding where the balance lies,
- Consult the DPO.

Reasons for disclosing or not disclosing will be reported to the Board of Trustees at the next committee meeting.

Where a statutory publication scheme duty applies, adopt the ICO model scheme and the relevant sector guidance. Otherwise, agree a proportionate voluntary publication approach. Publish appropriate information on our website to support transparency and accountability.

Apply charges only where permitted by the relevant legislation and an approved charging scheme, and issue any required notice. Do not automatically adopt Wakefield Local

Authority's charging regime. Confirm the charging arrangements with the DPO before approval.

Where applicable, respond to FOI requests promptly and normally within 20 working days, and EIR requests as soon as possible and within 20 working days, using only permitted extensions with timely notice and reasons. College holidays are not a general pause. The DPO must confirm any specific statutory variation that applies.

Internal Reviews

Provide a clear review route and check the applicable regime. EIR representations must normally be made within 40 working days of the alleged failure. For FOI, apply the adopted review procedure and current ICO guidance; do not treat the rules for the two regimes as identical.

A reviewer who was not involved in the original decision should reassess the handling and any withholding decision. Complete an FOI review normally within 20 working days, extending to no more than 40 in exceptional cases with reasons. Where EIR applies, communicate the review outcome as soon as possible and within 40 working days of receipt. These are working days, rather than college days.

If an individual remains dissatisfied after we have concluded our internal review they may appeal to the Information Commissioner's Office. Their contact details are below:

Phone: 0303 123 1113 or via their live chat. Their normal opening hours are Monday to Friday between 9am and 5pm (excluding bank holidays). You can also report, enquire, register and raise complaints with the ICO using their web form on Contact us | ICO.

Copyright

We will take reasonable steps to inform enquirers if any third party might have a copyright or intellectual property interest in information provided in response to their requests. However, it will be the enquirer's responsibility to ensure that any information provided by us is not re-used in a way which infringes those interests, whether or not any such warning has been given.

Camphill Wakefield

Appendix Four – Surveillance Policy

Introduction
This policy concerns our use of surveillance technology and related processing of personal data. It is written in accordance with data protection and human rights legislation and relevant codes of practice.

Surveillance is the close observation or monitoring of individuals or spaces, for the purpose of influencing behaviour or protecting people. We only use surveillance in the context of CCTV and e-monitoring. We do not operate covert surveillance technologies and therefore this policy does not cover the use of such technology.

CCTV
We operate Closed Circuit Television (CCTV) systems to:

- Protect college buildings and property
- Protect the safety and wellbeing of students, our workforce and visitors
- Deter and discourage anti-social behaviour such as theft and vandalism
- Support the police in the prevention, detection, investigation and prosecution of any crimes.

E-monitoring
We operate e-safety monitoring software systems to:

- Safeguard our students and staff
- Promote wellbeing and early intervention
- Ensure appropriate use of organisation assets and resources
- Monitor compliance with policies

Privacy Risk Assessment
Under the UK GDPR, we are required to consider and address privacy implications to data subjects when implementing new data processing systems. This is known as privacy by design. The usual method for assessing privacy risks to individuals is by carrying out a Data Protection Impact Assessment (DPIA).

A DPIA is mandatory for surveillance activities since they are deemed particularly intrusive. We will ensure that DPIAs have been completed for both CCTV and e-monitoring and that there are no unmitigated high risks to the rights and freedoms of data subjects. In addition, we will review and update the relevant DPIA if we substantively change our systems.

We will ensure we have completed the Privacy by Design checklist for call recording.

Contract Management
We are required to have contracts with any data processors we use, containing certain data processing clauses prescribed by law. We will ensure that we have implemented an appropriate contract with the providers of our CCTV and e-monitoring systems to allow for them storing, monitoring or accessing the data on our behalf. We will only agree to these

contracts where they have been assessed for compliance and determined to meet our requirements.

Transparency
The use of CCTV systems must be visibly signed. Signage will include the purpose of the system, the name of the organisation operating the system and details of who to contact about the system. The signage will be clear and kept unobstructed, so that anyone entering the area will be aware that they are being recorded.

The use of e-monitoring systems must also be clearly signed. Users will be made aware of the e-monitoring by a notice on the log in screen of computers and/or on the browser page when they join the network.

More detailed information about use of CCTV and e-monitoring must also be provided via a Privacy Notice, which must also inform data subjects about their rights in relation to their surveillance data. We have included the mandatory privacy information to data subjects in our relevant privacy notices.

Access Controls
Surveillance system data will only be accessed to comply with the specified purpose. For example, footage of CCTV systems intended to prevent and detect crime will only be examined where there is evidence to suggest criminal activity has taken place. Logs of e-monitoring systems intended to safeguard will only be examined where there is reasonable cause to believe someone is at risk.

Each system will have proportionate access controls and a nominated Information Asset Owner (IAO) who will be responsible for the governance and security of the system. The IAO may authorise other specified staff members to access data held on the systems routinely or on an ad-hoc basis.

Disclosures
A request by an individual for surveillance data held about them will be treated as a subject access request (SAR). For more information on data subjects' right of access to their information, please refer to our Data Protection Policy.

If we receive a request for surveillance data from an official agency, such as the police, then we will confirm the purpose of the request and their lawful basis for accessing the data. We may also require formal documentation in support of the request. We will liaise with our Data Protection Officer (DPO) if we have any concerns about such requests.

Record of Processing and Retention
We have a duty under Article 30 of the UK GDPR to ensure that all our data processing activities are recorded for accountability purposes. We maintain an Information Asset Register to fulfil this requirement. We will ensure that the use of surveillance systems is detailed on this register.

Surveillance records will only be held as long as necessary to fulfil the specific purpose and deleted in line with our Records Management Policy.

Reviews
CCTV systems must be reviewed annually to ensure that systems still comply with data protection legislation and national standards. The IAO should use the checklist included in Appendix A of this policy to complete this review.

The organisation will review the e-monitoring systems regularly by undertaking a review of the DPIA and updating the DPIA to reflect any changes in how the system is used or the type of data that is collected.

It is the responsibility of the relevant IAO to ensure reviews are completed and evidence of this is maintained.

Complaints
Complaints by individuals about the use of surveillance systems or data will be treated as a data protection concern. For more information on data protection complaints, refer to our main Data Protection Policy.

Appendix A – CCTV System Checklist

Camphill Wakefield:

Name and Description of Surveillance System:		
The purpose and requirements of the system are addressed by the system (i.e. the cameras record the required information).	**YES**	**NO**
	Notes:	
The system is still fit for purpose and produces clear images of adequate resolution.	**YES**	**NO**
	Notes:	
Cameras are sited in effective positions to fulfil their task.	**YES**	**NO**
	Notes:	
Cameras are positioned so that they avoid capturing the images of persons not visiting the premises and/or neighbouring properties.	**YES**	**NO**
	Notes:	
There are visible signs showing that CCTV is in operation. These signs include: ▪ Who operates the CCTV, ▪ Their contact details, ▪ What the purpose of the CCTV is.	**YES**	**NO**
	Notes:	
CCTV recordings are securely stored and access limited.	**YES**	**NO**
	Notes:	

The system has the capability to transfer recordings to law enforcement or to fulfil a request for an individual's own personal information.	**YES**	**NO**
	Notes:	
The system has a set retention period. This retention period should only be long enough to fulfil the CCTV's purpose and not longer. Outside of this retention period information should be deleted.	**YES**	**NO**
	Notes:	
The system users should be able to selectively delete information still inside the retention period to fulfil the right to erasure.	**YES**	**NO**
	Notes:	
All operators have been authorised by the Information Asset Owner and have sat their mandatory data protection training.	**YES**	**NO**
	Notes:	
The system has been added to the central record of surveillance systems.	**YES**	**NO**
	Notes:	

Checklist completed by:	**Checklist reviewed and signed by (Information Asset Owner):**
Name: Job Title: Date:	Name: Job Title: Date: