




DATA PROTECTION AND INFORMATION GOVERNANCE Corporate Policy


Title of Policy Document	Data Protection and Information Governance
Issue Date and Version	Version 3 (May 2024)
Policy Reference Number	
Has Equality Impact Assessment been completed?	
Categories	<input checked="" type="checkbox"/> Core <input type="checkbox"/> Corporate <input type="checkbox"/> Equal Opportunities <input type="checkbox"/> Health and Safety <input type="checkbox"/> Housing <input type="checkbox"/> Human Resources <input checked="" type="checkbox"/> Information Governance <input type="checkbox"/> IT and Communications <input type="checkbox"/> Learning and Development <input type="checkbox"/> Professional Practice and Standards <input type="checkbox"/> Recruitment <input type="checkbox"/> Service Management <input type="checkbox"/> Stakeholder Involvement <input type="checkbox"/> Support Planning and Risk Assessment <input type="checkbox"/> Service Provision – CQC services <input type="checkbox"/> Service Provision
Signed off by	 Chief Executive
First issue date	May 2018
Renewal date	May 2027

1. INTRODUCTION

- 1.1 Data is a vital asset to Creative Support, both in terms of the effective provision of care and support to individual service users, and the efficient management of services, resources and performance. It is therefore of paramount importance that the appropriate policies, procedures and management accountabilities are in place to provide a robust governance framework for information governance and data protection.
- 1.2 This policy sets out Creative Support's standards and expectations with respect to control and processing of personal data by employees relating to service users, employees and any other stakeholders.

2. LEGAL AND COMPLIANCE FRAMEWORKS

- 2.1 Data protection legislation in the UK is governed by the [Data Protection Act](#) (2018) and the "UK GDPR", the retained EU law version of the [General Data Protection Regulation \(EU\) 2016/679](#) as it forms part of UK law by virtue of section 3 of the [European Union \(Withdrawal\) Act](#) (2018) and as amended by Schedule 1 to the [Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2019](#) (SI 2019/419).
- 2.2 Practice covering the processing of personal information in social care is governed by the following legislation and guidance:
- [General Data Protection Regulation](#) (GDPR)
 - [Data Protection Act](#) (2018)
 - [Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations](#) (2019)
 - [Data Protection \(Processing of Sensitive Personal Data\) Order](#) (2000)
 - [Computer Misuse Act](#) (1990)
 - [Privacy and Electronic Communications \(EC Directive\) Regulations](#) (2003)
 - [The Caldicott Principles](#)
 - NHS and HSCIC Codes of Practice, including; [HSCIC Code of practice on confidential information](#) (2014) and [A Guide to Confidentiality in Health and Social Care](#) (2013)
 - [Human Rights Act](#) (1998)
 - [Public Records Acts](#) (1958 and 1967)
 - [Records Management Code of Practice for Health and Social Care](#) (DOH, 2016)
- 2.3 Creative Support is registered with the Information Commissioner's Office (ICO) under registration reference Z754770X. Service Director, Julie Cooke, is the named Senior Information Risk Owner (SIRO) and Caldicott Lead for the organisation. The certificate of ICO registration, which is renewed annually, is available for download from the Creative Support website.
- 2.4 Creative Support is obliged to comply with the NHS Information Governance standards for voluntary organisations as a social care provider that contracts with the NHS. Using the Data Security and Protection Toolkit (DSP) Creative Support will evidence its compliance with these standards, which incorporate the legislative requirements with respect to the secure processing of personal data. Annual submission of the DSP Toolkit is completed for all CQC registered services under the Headquarters code A7FE.

Data Protection and Information Governance	Version 3	Issued May 2024	Approved by: 
--	-----------	-----------------	---

- 2.5 Corporate responsibility for data protection and information governance is assumed by the following:

Senior Information Risk Owner (SIRO)

The SIRO for Creative Support is responsible for having overall accountability for Information Governance; this includes the data protection and confidentiality functions. The role includes briefing the Board of Trustees and providing assurance through the Finance and Audit Committee that the IG approach is effective, that all IG-related incidents are reported and followed up appropriately and that where appropriate reported through the DSP Toolkit. Creative Support is not legally required to have a Data Protection Officer but the SIRO fulfils this function.

Caldicott Lead

The Caldicott Lead has responsibility for ensuring that there are adequate standards for protecting service user information and that all data transfers are undertaken in accordance with Safe Haven guidelines and the Caldicott principles.

Head of Information Governance


The Head of Information Governance has day-to-day responsibility for implementing and monitoring procedures to ensure compliance with relevant information legislation, and reports directly to the SIRO/Caldicott Lead.

3. DEFINITIONS

- 3.1 Data protection legislation applies to “person identifiable information” (PII), i.e. *any data that can be used to identify an individual person*. This definition includes digital information (such as an IP address) and can also extend to pseudonymised data, where this can still be linked to an individual person.
- 3.2 A “data breach” occurs when a breach of security or procedure leads to the deliberate or accidental, unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data. This means that any incident in which PII is accessed or made available to parties who have no legal justification for doing so, may constitute a data breach. All such incidents must be reported in accordance with the procedure set out in section 7 below.
- 3.3 “Processing” or “processing activity” with respect to PII refers to any operation performed on personal data by an organisation and its employees that involves, but is not limited to, the collection recording, organisation, structuring, storage, editing, retrieval, disclosure, combination, restriction, erasure or destruction of that data.

4. PRINCIPLES OF DATA PROTECTION


- 4.1 As a social care provider and employer, Creative Support necessarily processes PII on its employees, service users and stakeholders. All such processing is subject to the [Data Protection Act](#) (2018) and is covered by this policy. Individuals identified in any of Creative Support’s processing activities have the following legal rights with respect to their own personal data:

Data Protection and Information Governance	Version 3	Issued May 2024	Approved by: 
--	-----------	-----------------	---

1. **The right to be informed** - Individuals have the right to be informed how and for what purposes their personal data will be processed.
 2. **The right of access** - Individuals have the right to access their personal data and supplementary information, and to be made aware of and verify the lawfulness of the processing.
 3. **The right to rectification** - Individuals have the right to have their personal data rectified if it is inaccurate or incomplete.
 4. **The right to erasure** - Also known as 'the right to be forgotten'. This is the right of individuals to request the deletion or removal of personal data where there are no compelling reasons for its continued processing.
 5. **The right to restrict processing** - Individuals have the right to permit the storing of their personal data, but to restrict any further processing; for example when an individual contests its accuracy.
 6. **The right to data portability** - Individuals have the right to obtain and reuse their personal data for their own purposes across different services.
 7. **The right to object** - Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interests/exercise of official authority (including profiling), direct marketing, and the processing of their personal data for purposes of scientific/historical research and statistics.
 8. **Rights in relation to automated decision making and profiling.** - These rights protect individuals from any automated decision making (i.e. decisions made solely by automated means without any human involvement, and profiling (i.e. automated processing of personal data to evaluate certain things about an individual).
- 4.2 Creative Support has issued comprehensive privacy statements to all [employees](#) and [service users](#), which explain how these rights will be protected, and the procedures that will be followed to ensure that the privacy of their personal data is protected at all times.
- 4.3 Creative Support's practice for the sharing of personal data with third parties when it is necessary to do so, is guided by the eight "Caldicott Principles", which are:
1. *Justify the purpose for using confidential information.*
 2. *Don't use personal confidential data unless absolutely necessary.*
 3. *Use the minimum necessary personal confidential data.*
 4. *Access to personal confidential data should be on a strictly need-to-know basis.*
 5. *Everyone with access to personal confidential data should be aware of their responsibilities.*
 6. *Understand and comply with the law.*
 7. *The duty to share information can be as important as the duty to protect patient confidentiality.*
 8. *Inform patients and service users about how their confidential information is used.*

5. LAWFUL BASES FOR PROCESSING PERSON IDENTIFIABLE INFORMATION

- 5.1 Creative Support use the following legal bases for the processing of PII:
- i. Pursuant to GDPR Article 6(1)(b) that the processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject prior to entering into a contract

Data Protection and Information Governance	Version 3	Issued May 2024	Approved by: 
--	-----------	-----------------	---

- ii. With respect to special categories of personal data, as defined in Article 9(1) of the GDPR, pursuant to GDPR Article 9(2)(h) that the processing is necessary for the provision of health or social care.
- iii. With respect to the processing of personal data relating to criminal convictions and offences, pursuant to Article 10, processing is authorised by State law; namely the UK [Data Protection Act \(2018\)](#), Schedule 1, that the processing 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, social security or social protection.
- iv. For all other information held, e.g. Ex-employee information, we will rely upon legitimate interests of the organisation pursuant to GDPR Article 6(1)(f).

5.2 “Special categories of personal data” are defined in Article 9 of the GDPR as relating to any of the following:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data for the purpose of uniquely identifying a natural person
- Data concerning health
- Data concerning a natural person’s sex life or sexual orientation

5.3 These categories of data will be processed when it is necessary to do so for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services. The legal bases for processing these special categories of employee and service user data specifically are detailed below.

5.4 Processing Special Categories of Employee Data

5.4.1 The special categories of personal data processed by Creative Support on its employees are; racial and ethnic origin, trade union membership, gender, and sexual orientation. Wherever employees or service users are asked to disclose such information about themselves, the right to withhold it from Creative Support will be made explicit to them at the point of collection, and this refusal will be recorded in the relevant data sets using “prefer not to say”, or equivalent terminology.

5.4.2 It is a legal requirement for Creative Support to submit information on its employees to the Skills for Care Workforce Data Set (WDS). Mandatory categories of data in the WDS include gender, ethnicity and nationality. For each of these categories of data an “unknown” option is available. Where individuals have chosen not to disclose this data, this option will be used.

5.4.3 As an employer committed to the promotion of equality and diversity, Creative Support will request the consent of employees to process information on their sexual orientation, gender identity or expression. The processing of this information will be for the purposes of promoting diversity through our status as a Stonewall “Diversity Champion”. Employees are under no legal or professional obligation, however, to disclose their sexual orientation, gender identity or expression to Creative Support, and their right to privacy in these matters will be respected and upheld. By default, these data will be recorded as “unknown” or “declined to disclose” unless the

information has been shared by the individual with their consent for them to be recorded.

- 5.4.4 Information on employees' trade union membership is accessed only by the Payroll department for the purposes of processing subscription fees, and may be disclosed to members of the Human Resources department in disciplinary or grievance cases where employees have been offered the opportunity for union representation.

5.5 Processing Special Categories of Service User Data

- 5.5.1 As a care provider, Creative Support processes a substantial amount of personal information on our service users, recognising that vulnerable adults divulge such information to professionals that is often sensitive and painful. Accordingly, Creative Support will ensure that such information is always treated with respect, upholding the service user's right to privacy, their personal dignity and protecting their best interests at all times.
- 5.5.2 Creative Support is lawfully permitted to process service user data pursuant to GDPR Article 9(2)(h) in that it is necessary to do so for the purposes of providing the services for which we are contracted, in order to fulfil our duty of care and to act in the best interests of individuals who may not always have the mental capacity to consent.
- 5.5.3 As a necessary component of providing holistic, personalised care services, Creative Support may collect sensitive data on our service users: in particular, racial or ethnic origin, political opinions, religious beliefs, data concerning health, and data concerning sex life and/or sexual orientation. What information is processed will vary relative to the identified care needs of each individual service user. Information that is not relevant to a service user's identified needs does not need to be recorded, and will not be recorded unless the service user gives their consent.

5.6 Additional Legal Bases for the Processing of Service User Information


- 5.6.1 There may be exceptional circumstances in which information will need to be shared with other professionals, where the conditions of GDPR Article 9(2)(h) do not apply. For example, when:

- A service user's life is considered to be at risk
- Other people's lives are considered to be at risk
- It is a requirement of a court order
- It is a requirement of law, or;
- It is in the public interest.

These circumstances are covered by Article 6, paragraph 1d and 1e of the GDPR, viz. "vital interests" and "public interest" respectively. **Safeguarding concerns always take priority over considerations of data protection.**

- 5.6.2 The main public interest justifications for the disclosure of health information – based on [National Health Service Confidentiality Code of Practice](#) (2003) and the [HSCIC Code of practice on confidential information](#) (2014) – are as follows:


- For public accountability and monitoring purposes.
- Serious risks to the health of other individuals.
- Serious risk to public health.

Data Protection and Information Governance	Version 3	Issued May 2024	Approved by: 
--	-----------	-----------------	---

- The reporting of adverse drug reactions.
 - The prevention, detection or prosecution of serious crime.
 - Disclosure to professional regulatory bodies (e.g. professional misconduct).
 - *Bona fide* and approved clinical/scientific research and surveys.
- 5.6.3 Any requests for information from an external agency on the grounds of public interest should be treated with care, discussed with senior managers and fully documented. Depending on the nature of the request and the information requested, it may be necessary to arrange a review meeting with the relevant agencies involved.
- 5.6.4 Where a request for disclosure is made in relation to a serious crime, the following conditions must be satisfied:
- The crime must be sufficiently serious for the public interest in disclosure to prevail over the individual's right to confidentiality.
 - It must be established that without the disclosure the task of preventing or detecting the crime would be seriously prejudiced or delayed.
- 5.6.5 There is no absolute definition of "serious crime". This policy therefore uses the definition of "serious arrestable offences" given in the [*Police and Criminal Evidence Act* \(1984\)](#) (section 116). These are offences that have caused or may cause:
- Serious interference with the administration of justice with the regard to the investigation of an offence.
 - Death.
 - Serious injury.
 - Substantial financial loss or gain.
- 5.6.6 The disclosure of information to the police in order to comply with Creative Support's *Alcohol and Misuse of Drugs* corporate policy is permissible with or without the express permission of the service user. If such information is to be shared this should only be done in consultation with a senior manager.
- 5.6.7 In the event of a worker being made aware of information relating to possible or actual physical, sexual, financial or emotional abuse of children or vulnerable adults, they must report their concerns immediately to their line manager, and the relevant Service Director or on-call manager. Their concerns will be dealt with within the agreed *Safeguarding Children and Young People* policy, or the *Safeguarding Adults* policy, and in line with corresponding Local Authority safeguarding procedures, to which reference should be made in the report. The safety of children and vulnerable adults should always be given the highest priority and should override considerations of confidentiality.
- 5.6.8 If any member of staff feels that any of the situations outlined above apply, then it is essential that they discuss the matter with their line manager, duty manager, or other senior member of staff.

6. DATA PROCESSING ACTIVITIES

- 6.1 Creative Support will observe procedures designed to protect PII data at every stage of its lifecycle, from receipt, through to processing, sharing, transfer, archiving and deletion. Employees who process personal data will ensure as part of every processing activity that:

Data Protection and Information Governance	Version 3	Issued May 2024	Approved by: 
--	-----------	-----------------	---

- a). Only the minimum necessary personal data is processed;
 - b). that anonymisation, pseudonymisation and granularisation are used wherever possible, and;
 - c). that processing is transparent (where feasible, allowing individuals to monitor what is being done with their data).
- 6.2 “Pseudonymisation” refers to the use of other identifying data in place of individuals’ names (such as an employee number) where it is not necessary for that processing activity to disclose names, e.g. for the purposes of compiling reports or statistical information. Employees must “granularise” sets of personal data pertaining to ten or more individuals when these are being shared in any format (digital or hard copy). Large spreadsheets, lists and any other such sets of data should be broken down into smaller units such that any one transfer does not include information on more than ten individuals.

6.3 Processing Service User Data

- 6.3.1 Creative Support keeps individual files for each service user, which the staff are responsible for maintaining in accordance with the legal bases as set out in section 5 above. Information in service user files will be maintained with consideration of the rights of the individual to their personal data as outlined in section 4.1 above.
- 6.3.2 Services using digital/online systems for processing service user data will follow the *ICT Security* and related policies to ensure that access to service user data is secured. In 2024, Creative Support is launching the “ECCO” electronic system for all service user care notes. As services are onboarded on to ECCO, hard copies of paper-based care notes will be archived in accordance with the *Management and Archiving of Records* policy. The same procedure will be applied for any other digital systems used in specific services where these replace paper-based records.
- 6.3.3 The confidentiality of service user records must be respected and maintained at all times. Paper files must not be left open on desks or around the office, and must be stored in a lockable cabinet when not being used. Digital files must be stored securely in accordance with the corporate [ICT Security](#) and related policies. Access to service user data will be on a “need to know” basis within Creative Support. The standard purposes for which an employee will need access to personal service user data will be either:
- a). The employee is professionally involved with providing care or support to the service user, either as a care worker or a manager of the service that provides the service to that individual, or;
 - b). The employee is involved with any corporate procedures that require access to PII for the purposes of safeguarding, quality assurance, data analysis, governance or oversight of services at the senior management level.
- 6.3.4 Employees who meet neither of the above criteria will be granted access to service user data only if it necessary for them in order to provide the service for which Creative Support is contracted. Where anonymised or pseudonymised data fulfils the same purpose, data will be accessed by those employees in those formats. The same will apply to external stakeholders who require access to data for inspection and auditing purposes (such as CQC, local authorities, and commissioning bodies).
- 6.3.5 The loss or theft of personally identifiable service user data may constitute a data breach that is reportable to the Information Commissioner’s Office (ICO). Any such


incident must be reported using a standard Creative Support incident report to the Information Governance team at ig@creativesupport.co.uk and incidents@creativesupport.co.uk as soon as possible and always within 72 hours of the incident occurring. Where the data cannot be or has not been recovered, the Information Governance team will report such incidents through the DSP Toolkit, which determines whether the incident is reportable to the ICO.

6.4 Processing Employee Data

- 6.4.1 Creative Support uses the iTrent platform as its main repository of employee data, for storing and processing those data in accordance with the legal bases as set out in section 5 above. Information in employee files will be maintained with consideration of the rights of the individual to their personal data as outlined in section 4.1 above.
- 6.4.2 The confidentiality of employee records must be respected and maintained at all times. Paper files must not be left open on desks or around the office, and must be stored in a lockable cabinet when not being used. Digital files must be stored securely in accordance with the corporate [ICT Security](#) and related policies. Access to employee data will be on a “need to know” basis within Creative Support. The standard purposes for which an employee will need access to personal employee data will be either:
- a). The employee accessing the data is professionally involved with managing a service at which the employee data subject works, or;
 - b). The employee accessing the data is involved with any corporate procedures that require access to PII for supervision/line management, HR, payroll, governance or other purposes at the senior management level.
- 6.4.3 Sick notes (“fit notes”) are confidential documents and should be submitted to the payroll email addresses, Notifications.MonthlyPayroll@creativesupport.co.uk, weekly.payroll@creativesupport.co.uk, or bank.payroll@creativesupport.co.uk as appropriate. Information disclosed in “fit notes” is treated confidentially in accordance with this policy and related legislation.
- 6.4.4 Enquiries from statutory authorities for information about staff (e.g. Police), should always be referred to the Human Resources Department or the relevant senior manager/Service Director.
- 6.4.5 Creative Support uses the Disclosure & Barring Service (DBS) to help assess the suitability of applications for positions of trust. Creative Support complies fully with the [DBS codes of practice](#) and related recruitment requirements.
- 6.4.6 Disclosure information is never kept on an applicant’s personnel file and is destroyed once the result of the check has been recorded on. We use the online “Care Check” service for processing DBS applications. This service is fully compliant with GDPR: please refer to <https://www.carecheck.co.uk/wp-content/uploads/2021/01/gdpr-policy.pdf> for more information.

7. REPORTING DATA BREACHES

- 7.1 Data breaches, as defined in 3.2 above must be reported following Creative Support’s Incident Reporting policy, and emailed to ig@creativesupport.co.uk as soon as possible, and always within 72 hours of the breach being identified. The report must include the following information:

Data Protection and Information Governance	Version 3	Issued May 2024	Approved by: 
--	-----------	-----------------	---

- What data has become available, and to whom
 - How many data subjects (individual people) have been affected by the breach
 - How and why the breach occurred
 - What measures have been taken to contain the breach
- 7.2 When an accidental breach is identified, the priority must be to contain the breach by identifying how and why the data was shared with the unauthorised party, and then contacting that party directly to ask them to delete or destroy the data. Once this has been achieved, the breach can be said to have been contained. Where it has not been possible to contain the breach, this fact must be included with the incident report, and the relevant senior manager notified in person of what has occurred at the earliest opportunity.
- 7.3 Serious data breaches, including those believed to be intentional or malicious, or those involving a large amount of personal data, must be notified to the SIRO/Caldicott Guardian immediately.
- 7.4 In the interests of transparency, the affected data subjects must be notified of the breach, and an apology issued on behalf of Creative Support, along with information regarding how to make a complaint, either through the internal complaints procedure, or externally to the ICO.
- 7.5 All incidents involving data breaches that have not been immediately contained, or which may put individuals at risk of further harm due to their data being accessible to unauthorised parties, will be reported through the DSP Toolkit. Reporting breaches through this system automatically notifies the ICO of the incident when it meets their threshold of severity. Incidents notified to the ICO in this way are subject to their own investigation procedure.
- 8. RETENTION AND DELETION**
- 8.1 All records of Creative Support employees and service users will be retained in accordance with the corporate *Management and Archiving of Records* policy. The standard retention period for these records is eight years after the end of employment (for employees) or after the end of service (for service users). Please refer to the separate corporate policy for more information.