




# DATA PROTECTION AND INFORMATION GOVERNANCE Corporate Policy


<b>Title of Policy Document</b>	<b>Data Protection and Information Governance</b>
<b>Issue Date and Version</b>	<b>Version 2 (May 2021)</b>
Policy Reference Number	6
Has Equality Impact Assessment been completed?	N/A
Categories	<ul style="list-style-type: none"><li><input checked="" type="checkbox"/> Core</li><li><input type="checkbox"/> Corporate</li><li><input type="checkbox"/> Equal Opportunities</li><li><input type="checkbox"/> Health and Safety</li><li><input type="checkbox"/> Housing</li><li><input type="checkbox"/> Human Resources</li><li><input checked="" type="checkbox"/> Information Governance</li><li><input type="checkbox"/> IT and Communications</li><li><input type="checkbox"/> Learning and Development</li><li><input type="checkbox"/> Professional Practice and Standards</li><li><input type="checkbox"/> Recruitment</li><li><input type="checkbox"/> Service Management</li><li><input type="checkbox"/> Stakeholder Involvement</li><li><input type="checkbox"/> Support Planning and Risk Assessment</li><li><input type="checkbox"/> Service Provision – CQC services</li><li><input type="checkbox"/> Service Provision</li></ul>
Signed off by	 Chief Executive
Renewal date	May 2024
First issue date	May 2018

## 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.

## 2. LEGISLATIVE FRAMEWORK

- 2.1 The European Union's *General Data Protection Regulation* (GDPR) came into force, along with the UK's [Data Protection Act](#) on 25<sup>th</sup> May 2018. Concurrent with the UK's exit from the European Union on 1<sup>st</sup> January 2021, the [Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations](#) (2020) came into effect, merging the requirements of the EU GDPR to form a new, UK specific data protection regime that works in a UK content as part of the [Data Protection Act](#) (2018).
- 2.2 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.
- 2.3 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)
- 2.4 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.
- 2.5 This policy sets out the legal and corporate framework for the protection of all personal data processed by Creative Support, relating to service users employees, and stakeholders, in accordance with the legislative framework as detailed in 2.1 – 2.4 above.

Data Protection and Information Governance	Version 2	Issued May 2021	Approved by: 
--	-----------	-----------------	---

### 3. CORPORATE RESPONSIBILITY FOR DATA PROTECTION AND INFORMATION GOVERNANCE

#### 3.1 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.

#### 3.2 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.

#### 3.3 Information Governance Lead

The Information Governance Lead 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.

### 4. PERSONALLY IDENTIFIABLE INFORMATION

4.1 “Personal data”, or “personally identifiable information” (PII) is defined as any data that can be used to identify an individual person, either on its own or in conjunction with other accessible data on that individual. 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.


4.2 As a social care provider and employer, Creative Support processes PII on its employees and its service users. The control and processing of all such data is regulated by the [Data Protection Act](#) (2018).

4.3 All systems used for the control and processing of personal data are subject to a process of Data Protection Impact Assessment (DPIA).

### 5. PRINCIPLES OF DATA PROTECTION

5.1 Under the [Data Protection Act](#) (2018) all individuals have the following rights in relation to their PII:


- i. **The right to be informed** - Individuals have the right to be informed how and for what purposes their personal data will be processed.
- ii. **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.
- iii. **The right to rectification** - Individuals have the right to have their personal data rectified if it is inaccurate or incomplete.

Data Protection and Information Governance	Version 2	Issued May 2021	Approved by: 
--	-----------	-----------------	---

- iv. **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.
  - v. **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.
  - vi. **The right to data portability** - Individuals have the right to obtain and reuse their personal data for their own purposes across different services.
  - vii. **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.
  - viii. **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).
- 5.2 Creative Support has issued comprehensive privacy statements to all [employees](#) and [service users](#), which explain how their 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. These are available to download via <https://www.creativesupport.co.uk/privacy-policy> and in the staff area of the Creative Support website.
- 5.3 Privacy statements will be available to every employee as part of the recruitment and selection process, and to every service user at the point of referral. The terms of privacy statements apply to potential employees at the point of application, and to service users at the point of referral, in so far as it is necessary to process their personal data in order to carry out the recruitment/assessment processes.
- 5.4 Creative Support will practice “data protection by design”, such that any employee processing PII will ensure that:
- Only the minimum necessary personal data is processed
  - That anonymization, pseudonymization and granularisation are used wherever possible
  - That processing is transparent (where feasible, allowing individuals to monitor what is being done with their data)
- 5.5 “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 more than ten 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. This applies even if the data has also been pseudonymised. Please refer to the [Personal and Sensitive Data](#) policy for more information on good data protection practice.

## 6. LAWFUL BASES FOR PROCESSING DATA

- 6.1 The GDPR (Article 6) requires data controllers to specify their lawful basis for processing of personal data. Whereas Creative Support previously processed personal data on the basis of consent, with service users and staff having given their

Data Protection and Information Governance	Version 2	Issued May 2021	Approved by: 
--	-----------	-----------------	---

express permission for us as a social care provider/employer to do so, under the GDPR (Article 7 and Recital 43), it is no longer permissible to do so when this is given as a condition for the provision of a service or employment. This is because the consent cannot be regarded as freely given, where there is a clear imbalance between the data subject and the controller, as exists between Creative Support and its employees and service users.

6.2 As of 25<sup>th</sup> May 2018 Creative Support will, therefore, use the following legal bases for the processing of personal data:

- 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
- 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).

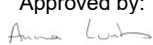
6.3 “Special categories of personal data” are defined in Article 9 of the GDPR as relating to any of the following:

- 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

6.4 In accordance with 6.2 and 6.3 above, 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.

## 6.5 Processing Special Categories of Employee Data

6.5.1 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.

Data Protection and Information Governance	Version 2	Issued May 2021	Approved by: 
--	-----------	-----------------	---


- 6.5.2 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.
- 6.5.3 As an employer committed to the promotion of equal opportunities, Creative Support will request the consent of employees to process information on their sexual orientation, gender identity or expression, should they choose to disclose it. The processing of this information will be for the purposes of promoting equal opportunities 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.
- 6.5.4 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.

## 6.6 Processing Special Categories of Service User Data

- 6.6.1 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.
- 6.6.2 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.
- 6.6.3 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.

## 6.7 Additional Legal Bases for the Processing of Service User Information

- 6.7.1 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.

Data Protection and Information Governance	Version 2	Issued May 2021	Approved by: 
--	-----------	-----------------	---

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.**

6.7.2 The main public interest justifications for the disclosure of health information – based on [National Health Service Confidentiality Code of Practice](#) (2003) – are as follows:

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

6.7.3 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.

6.7.4 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.

6.7.5 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 which 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.

6.7.6 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.

6.7.7 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.

Data Protection and Information Governance	Version 2	Issued May 2021	Approved by: 
--	-----------	-----------------	---




- 6.7.8 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.

## 7. PRINCIPLES OF PRIVACY AND CONFIDENTIALITY

Sections 7.1 and 7.2 below should be read with reference to the corporate [Personal and Sensitive Data](#) policy.

### 7.1 Service User Data

- 7.1.1 Creative Support keeps individual files for each service user, which the staff supporting the service user are responsible for maintaining. Information in service user files will be maintained with consideration of the rights of the individual to their personal data as outlined in section 5.1 above, and archived in accordance with the organisation's [Management and Archiving of Records](#) policy.
- 7.1.2 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. (A corporate policy covering the use of online systems is forthcoming).
- 7.1.3 Service user files should not be removed from the secure office location in which they are usually stored, except in exceptional circumstances. In such cases, the agreement of a senior member of staff must be sought before removing files from their usual location. If removing a file, copies of the front sheets or 'grab sheets' detailing essential information should be retained, so that staff working with the service user will have access to such information in the event of an emergency.
- 7.1.4 Services will have procedures in place to ensure there is an auditable "paper trail" that records any movement of files to or from their usual location. These will allow for the recording of what documents were moved, by whom, and when; such that an investigation in the event of data breach can be meaningfully conducted.
- 7.1.5 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](mailto:ig@creativesupport.co.uk) and [incidents@creativesupport.co.uk](mailto: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.
- 7.1.6 The confidentiality of service user files 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.
- 7.1.7 As a point of practice, letters and other information from external agencies (known as "third party information") should be immediately filed after reading. Third party information must be accessible to the relevant members of staff and should not be stored in places other than the main service user file.
- 7.1.8 Access to a service user's file is limited to the support worker(s), their line manager or those members of staff who are directly involved in the support of the service user, or

Data Protection and Information Governance	Version 2	Issued May 2021	Approved by: 
--	-----------	-----------------	---




to Creative Support employees involved in the auditing of the service; and in the case of local authority or CQC inspections, to the professionals carrying those processes, as governed by their own confidentiality and data protection policies.

- 7.1.9 If a service user approaches staff expressing information of a personal nature, they should be offered a private space in which to discuss this, and assured that personal information does not need to be given in a public area if they are not comfortable doing this.
- 7.1.10 Where possible, telephone calls should be passed directly to the member of staff who would most appropriately deal with the enquiry. If this is not possible, then a message should be taken, and passed to the member of staff in question. If a call is urgent and the relevant member of staff is not available, brief details should be taken, and then referred to the relevant line manager, local on call, or other senior member of staff. Service users who phone an office should be made aware that they do not have to give personal information over the phone, especially if they cannot speak to the person dealing with their case.

## 7.2 Employee data

- 7.2.1 Supervision files in services must be kept in a locked filing cabinet, with access restricted to the line manager, service manager and relevant administrative staff where appropriate.
- 7.2.2 Staff personal contact details must not be kept in any accessible phone books or card indexes on view in the service. If an emergency call comes in for a member of staff, the person taking the call should take the message and contact the person concerned directly. If enquiries are made about a member of staff, the enquirer's name should be taken and the member of staff informed. Staff are instructed never to give out staff or telephone numbers or addresses where there is doubt as to the enquirer's identity, or as to whether the individual has consented to their personal information being shared. If staff have any doubts as to what action they should take, they should pass the query to their line manager or a member of the Human Resources Team during normal office hours, or to the relevant on call or the Out of Hours service at any other time. Personal contact details of employees should be shared strictly on a "need to know" basis, and not made available to colleagues without the explicit consent of the individual.
- 7.2.3 Sick notes ("fit notes") are confidential documents and should be submitted to the payroll email addresses, [Notifications.MonthlyPayroll@creativesupport.co.uk](mailto:Notifications.MonthlyPayroll@creativesupport.co.uk), [weekly.payroll@creativesupport.co.uk](mailto:weekly.payroll@creativesupport.co.uk), or [bank.payroll@creativesupport.co.uk](mailto:bank.payroll@creativesupport.co.uk) as appropriate. Information disclosed in "fit notes" is treated confidentially in accordance with this policy and related legislation.
- 7.2.4 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.
- 7.2.5 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.
- 7.2.6 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:

Data Protection and Information Governance	Version 2	Issued May 2021	Approved by: 
--	-----------	-----------------	---

please refer to <https://www.carecheck.co.uk/wp-content/uploads/2021/01/gdpr-policy.pdf> for more information.

## 8. SUBJECT ACCESS REQUESTS

8.1 Creative Support is committed to working in an open and honest manner with our service users and employees. As per Article 15 and Recital 63 of the GDPR, data subjects have, “the right of access to [their] personal data...and to exercise that right easily and at reasonable intervals, in order to be made aware of, and verify, the lawfulness of the processing”. Accordingly, Creative Support will respond to all requests for personal data within one calendar month of receipt, as described below.

### 8.2 Employee Data

8.2.1 Employees may request to see their personal data that is processed by Creative Support, and to know the organisation’s reasons for doing so. This is called a “subject access request”, which an employee can make by submitting a [Subject Access Request for Creative Support Employees](#) form.

8.2.2 Information requested by the employee will be provided as soon as possible and no later than one month after the receipt of the form named above. If the employee has any special communication needs, we will endeavour to provide the information you have requested in an accessible format (e.g. providing large print copies for those with impaired sight). Creative Support reserves the right to provide data electronically using a secure (time limited) file sharing service instead of by post. This is to minimise the risk of loss in transit of personal data through third party.

8.2.3 Employees making subject access requests should specify when making their request specifically which items of personal data it is they wish to see.


8.2.4 There will be no charge to the employee for making a subject access request, unless the request is manifestly unfounded, excessive or repetitive, in which case a fee may be charged.

8.2.5 Creative Support began processing employee data, using the iTrent cloud platform in April 2018, which allows individual employees securely to access their personal data controlled by Creative Support. Employees will be able to access their personal data to confirm its accuracy, to rectify any errors or update changes as they occur. Employees should note that if requesting personal data dating back prior to April 2018, it may take longer to process their request.

8.2.6 Confidential references received by Creative Support are not exempt from data subject access requests. However, in deciding whether to disclose information, it is necessary also to consider the data privacy rights of the referee. Information contained in or about a confidential reference need not be provided if the release of the information would identify an individual referee unless:

- The referee has given his or her consent
- The identity of the referee can be protected by anonymising the information
- It is reasonable in all the circumstances to release the information without consent.

8.2.7 Even if a referee states that they do not want their comments to be shared, we are obliged to provide the reference to the subject if it is reasonable in all the circumstances to comply with the request without the referee’s consent. In considering whether it is

Data Protection and Information Governance	Version 2	Issued May 2021	Approved by: 
--	-----------	-----------------	---

reasonable, the Information Commissioner's Office (ICO) advises that, as data controllers, we should take account of factors such as:


- Whether the referee was given express assurances of confidentiality
  - Any relevant reasons the referee gives for withholding consent
  - The potential or actual effect of the reference on the individual
  - The fact that a reference must be truthful and accurate and that without access to it the individual is not in a position to challenge its accuracy
  - That good employment practice suggests that an employee should have already been advised of any weaknesses
  - Any risk to the referee.
- 8.2.8 Creative Support cannot refuse to disclose information from a confidential reference without giving a reason.
- 8.2.9 If disclosure of a reference would identify only the organisation that has given the reference rather than a specific individual, disclosure would not be an issue.
- 8.2.10 If a subject access request is received for information contained in a confidential reference that has been sent or received internally, it will be treated in the same way as a reference from an external referee. Internal references are not exempt from data subject access.

### 8.3 Service User Data


- 8.3.1 Service users may access their personal data by submitting a Subject Access Request. They may do so in any written form, whether this is by submitting a [Subject Access Request for Creative Support Service Users](#) form, by email, letter or other written notification made to a Creative Support employee.
- 8.3.2 Third party information, including information made available verbally and subsequently recorded, can be shared with service users, only with the explicit consent of the originator of that information, which should be in writing and should specify exactly with whom the information can be shared. Where no such consent has been given and can be evidenced, all information identifying the third party must be redacted before the information is disclosed to the service user.
- 8.3.3 In certain circumstances it may be not be appropriate to disclose all or part of the information that a service user has requested, such as; where the individual could be put at risk by sharing information, or where in the opinion of a professional involved in their care (e.g. a psychiatrist or social worker) to do so might negatively impact on their mental health or wellbeing. While every effort will be made to uphold the individual's rights to access their personal data, considerations of their best interests may override this.

## 9. SHARING PERSONALLY IDENTIFIABLE INFORMATION WITH THIRD PARTIES.

- 9.1 In the processing and sharing of service user and employee data with other professionals, Creative Support is guided by the seven "Caldicott Principles" as given in the *Report on the Review of Patient-Identifiable Information* (DOH, 1997) and the subsequent report, *The Information Governance Review: To Share or Not to Share* (DOH, 2013). These principles are:

Data Protection and Information Governance	Version 2	Issued May 2021	Approved by: 
--	-----------	-----------------	---

- **Principle 1 - Justify the purpose(s) for using confidential information.** Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.
  - **Principle 2 - Don't use personal confidential data unless it is absolutely necessary.** Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).
  - **Principle 3 - Use the minimum necessary personal confidential data.** Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.
  - **Principle 4 - Access to personal confidential data should be on a strict need-to-know basis.** Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.
  - **Principle 5 - Everyone with access to personal confidential data should be aware of their responsibilities.** Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.
  - **Principle 6 - Comply with the law.** Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.
  - **Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality.** Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.
- 9.2 All requests made to Creative Support employees regarding service users should be considered in the light of the Caldicott principles. **It is essential that employees understand that safeguarding considerations always take priority over matters of data protection.**
- 9.3 When requests for service user information are made verbally, the third party should be asked for their full name, job title, phone number and office location, and for the precise reason for requesting such information. If any doubt as to what is the appropriate action to take, staff should seek guidance from their supervisor, site manager, on call service or other senior member of staff. Before divulging any information, staff should take care to identify the caller (for example, by ringing back a social worker - having checked the authenticity of the phone number - or by checking the person's identity with a duty manager of the social worker's office). These steps should take only a few minutes and should not obstruct enquiries of an urgent nature. Most professionals and agencies will understand and respect the member of staff who politely explains the need to work within the law and the terms of Creative Support policy in this regard.
- 9.4 All police requests for information regarding a service user should immediately be referred to the staff member's line manager, on call service, or the Out of Hours service. In some cases it will be appropriate for the line manager to consult with other professionals involved in the service user's care (e.g. consultant psychiatrist or social worker) before making a decision as to whether information should be disclosed. Refer to the corporate policy, [Responding to Police Enquiries](#) for more information.

Data Protection and Information Governance	Version 2	Issued May 2021	Approved by: 
--	-----------	-----------------	---

## 10. PRINCIPLES OF INFORMATION GOVERNANCE

10.1 Creative Support recognises the need for an appropriate balance between openness and confidentiality in the management and use of information, while seeking to work within the legal framework as outlined in this policy. Creative Support recognises the duty to share accurate information with other health organisations and other agencies in a secure and legally compliant manner consistent with the interests of employees and service users, and in some circumstances, the public interest. Equally important is the need to ensure high standards of data protection and confidentiality to safeguard personal and sensitive (including commercially sensitive) information. Underpinning this is the integrity needed for electronic and paper information to be accurate, relevant, and available to those who need it.

10.2 Staff must ensure at all times that high standards of data quality, data protection, integrity, confidentiality and records management are met in compliance with the relevant legislation and guidance. It is the responsibility of all staff to familiarise themselves with this policy and adhere to its principles.

10.3 There are four key interlinked strands to Information Governance:

- Openness
- Legal Compliance
- Information Security
- Quality Assurance

### 10.4 Openness

10.4.1 Non-confidential information on Creative Support and its services will be made available to the public through a variety of media.

10.4.2 Creative Support does not meet the definition of a “public authority” under the [Freedom of Information Act](#), and as such is not subject to freedom of information requests.

10.4.3 Service users will be able to exercise their right to access information relating to their own health and social care and their rights as service users using subject access request procedures as described in section 8 above.

10.4.4 Creative Support will have clear procedures and arrangements for liaison with the press and broadcasting media.


10.4.5 Creative Support will have clear procedures and arrangements for handling queries from service users, the public, and other parties.

### 10.5 Legal Compliance

10.5.1 Creative Support regards all identifiable personal information relating to service users as confidential.

10.5.2 Creative Support regards all identifiable personal information relating to staff as confidential except where legislation on accountability and openness requires otherwise.

10.5.3 Creative Support will establish and maintain policies for the control and appropriate sharing of service user information with other agencies, taking account of relevant

Data Protection and Information Governance	Version 2	Issued May 2021	Approved by: 
--	-----------	-----------------	---

legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act).


- 10.5.4 In the handling of personal data on employees and service users, Creative Support employees are bound by the common law duty of confidentiality, i.e. any personally identifiable information disclosed to employees should not be shared where to do so would be unfair, or unnecessary.

## 10.6 Information Security

- 10.6.1 Creative Support will maintain policies for the effective and secure management of its information assets and resources. This will include a record of processing activities for all transfers of personally identifiable information from or to the organisation's Head Office departments. Managers in services are also expected to have oversight of how information is communicated within and outside of the organisation.
- 10.6.2 Creative Support will promote effective confidentiality and security practice to its staff through policies and training.
- 10.6.3 Creative Support will undertake an annual review of its information security and business continuity arrangements and this will be reported to the Board of Trustees.
- 10.6.4 Creative Support will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security. Creative Support will ensure all IG incidents which are assessed as potential data breaches and are reported through the Data Security and Protection (DSP) Toolkit. The DSP Toolkit assess whether incidents reported through their portal are sufficiently serious to warrant notification to the Information Commissioner's Office (ICO). When this is the case, the incident logged with the DSP is notified to the ICO automatically, who may then conduct their own investigation.
- 10.6.5 The Information Governance team have created a Confidentiality and Security Audit Tool that managers in services may use as a self-assessment to determine that the procedures in place locally are sufficient to ensure security of data held onsite, in either paper or digital format.

## 10.7 Information Quality Assurance

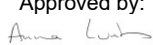
- 10.7.1 Creative Support will maintain policies and procedures for information quality assurance and the effective management of records. These include the [Management and Archiving of Records](#) policy and the [Personal and Sensitive Data](#) policy.
- 10.7.2 Managers are expected to take ownership of, and seek to improve, the accuracy and quality of information within their services, with due regard to the information functions and service delivery requirements. It is expected that managers in services will routinely audit service user and staff information stored locally for accuracy, consistency and relevance.
- 10.7.3 Wherever possible, information quality should be assured at the point of collection. Data standards will be set through clear and consistent definition of data items, in accordance with national standards. Creative Support will promote information quality and effective records management through policies, procedures/user manuals and training. Refer to the separate [Personal and Sensitive Data](#) policy for more details.

Data Protection and Information Governance	Version 2	Issued May 2021	Approved by: 
--	-----------	-----------------	---



## 11. INFORMATION GOVERNANCE MANAGEMENT

- 11.1 The framework for the management of Information Governance combines both corporate and clinical governance, and as such is wider in scope than data protection, also incorporating records management, information risk, information security, risk management, and business continuity.
- 11.2 The Information Governance Lead submits its self-assessment for compliance with the Data Security and Protection (DSP) Toolkit standards on an annual basis. This submission is completed on behalf of the entire organisation under Headquarters code A7FE, covering all CQC registered services. Further information on each of these standards is available at the DSP Toolkit website at <https://www.dsptoolkit.nhs.uk/>
- 11.3 The DSP Toolkit will be used by Creative Support to conduct a baseline audit and construct action plans to ensure future IG compliance and continuous improvement. The work programmes in individual areas will be created by adherence to the DSP standards and to the national standards appropriate to the specific field of activity.

Data Protection and Information Governance	Version 2	Issued May 2021	Approved by: 
--	-----------	-----------------	---