Data Protection Policy

To be considered in conjunction with The Caldecott Foundation's online policies and procedures.

In the event that anything in this policy conflicts with any other policy on matters of data protection then this policy should be taken to override the other.

The Caldecott Foundation complies with UK Data Protection Legislation and is registered as a 'Data Controller' with the Information Commissioner's Office (Reg. No. Z5860485).

The Data Protection Officer (DPO) is GRCI Law.

We ensure that personal data is processed fairly and lawfully, is accurate, is kept secure and is retained for no longer than is necessary.

Author: *Timothy Allison, HR & Business Manager (DPO)*, 5th October 2022

Reviewed by the Board of Trustees, 20th October 2022

INTRODUCTION

- The Caldecott Foundation is required to keep and process certain information about its staff members, young people and donors in accordance with its legal obligations under the EU General Data Protection Regulation (GDPR), the UK

GDPR, the Data Protection Act 2018 and other relevant UK laws and regulations.

- We may, from time to time, be required to share personal information about our staff, young people or donors with other organisations, such as placing local authorities, statutory bodies, other schools and the other organisations.
- This policy is in place to ensure all staff, governors and Trustees are aware of their responsibilities and outlines how the organisation complies with the relevant data protection laws and regulations.

PERSONAL DATA

- Personal information is any information that relates to a living individual who can be identified from the information. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.
- Personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier or an IP address. This applies to both computerised personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.
- Sensitive personal data is referred to in the UK GDPR as 'special categories of personal data'. These specifically include the processing of genetic data, biometric data and data concerning health matters.
- In the provision of its services The Caldecott Foundation collects personal data in relation to staff, volunteers, young people, the parents, carers and guardians of young people and donors. In addition, it may be required by law or contract to collect and use certain types of information to comply with statutory obligations of placing local authorities, government agencies and other bodies and organisations.

LEGAL FRAMEWORK

This policy has due regard to legislation, including, but not limited to the following:

- The EU General Data Protection Regulation (GDPR)
- The UK GDPR
- The Data Protection Act 2018
- The Children's Homes Regulation (England) 2015
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The School Standards and Framework Act 1998

PRINCIPLES

In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.

- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

ACCOUNTABILITY

- The Caldecott Foundation takes technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR. It provides privacy notices to inform data subjects about how their data is used. Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

DATA PROTECTION OFFICER (DPO)

The DPO:

- monitors the organisation's compliance with relevant data protection laws and regulations.
- reports directly to the Board of Trustees which is the highest level of management.
- will not be dismissed, disciplined or penalised for performing their duties.

LAWFUL PROCESSING

Under the GDPR, data will be lawfully processed where it is necessary for:

- Compliance with a legal obligation.
- For the performance of a contract with the data subject or to take steps to enter into a contract.
- The performance of a task carried out in the public interest.

- Protecting the vital interests of a data subject or another person.
- Meeting the legitimate interest of the data subject, the organisation or another person.
- The consent of the data subject has been obtained.

Special Category data (Sensitive Personal) data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by law.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is required to meet the legitimate interest of the data subject, the organisation or another person.
- Carrying out obligations under employment.
- Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
- The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.

CONSENT

- Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.
- Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.
- Where consent is given, a record will be kept documenting how and when consent was given.
- The Caldecott Foundation ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.
- Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.
- Consent can be withdrawn by the individual at any time.
- Where consent is the legal basis for processing a child's data, consent of a child's parents or legal guardian will be sought prior to processing.

DATA SUBJECT RIGHTS

Any one of the rights set out below may be passed to any staff, governor or Trustee by any method. In the event of receiving such a request you should record as much information as possible and then inform Timothy Allison, HR & Business Manager or Jonathan Butler Data Protection & IT Officer as soon as possible.

THE RIGHT TO BE INFORMED

- The privacy notice supplied to individuals in regard to the processing of their personal data is written in clear, plain language which is concise, transparent, easily accessible and free of charge.
- Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.
- Where data is not obtained directly from the data subject, information regarding the source the personal data originates from and whether it came from publicly accessible sources, will be provided.
- For data obtained directly from the data subject, a privacy notice will be available at the time the data is obtained and will provide this information.

THE RIGHT OF ACCESS

- Individuals have the right to obtain confirmation that their data is being processed.
- Requests for information held on another person other than the requesting individual or their children will not be provided unless full written consent has been given by the individual(s) in question, their next of kin or an individual who hold power of attorney. Prior to seeking consent advice would be taken from our DPO.
- Individuals have the right to submit a Data Subject Access Request (DSAR) for copies of their personal data that we are processing.
- DSARs do not need to be made using the organisation's template SAR form. If the initial request does not clearly identify the information required, then further enquiries will be made.
- All DSARs will be passed to the Manager responsible for data protection who will make the final decision on all requests. Advice may be sought from our DPO.
- In line with the legislation The Caldecott Foundation will verify the identity of the person making the request before any information is supplied. If the request relates to a child and the person requesting is a parent, carer or guardian then checks will be carried out to establish proof of the relationship.

- Third party information is that which has been provided by another organisation or individual such as the Police, Local Authority or Health care professional. Before disclosing third party information consent should normally be obtained.
- If information is anonymised or redacted (blacked out / removed) then a full copy of the information will be retained in order to establish, in the event of a complaint, what was anonymised. A record should be keep detailing the reasons for anonymising or redacting information.
- If there are concerns over any disclosure of information, perhaps because it may serious harm then additional advice should be sought from the DPO before disclosure.
- A copy of the information will be supplied to the individual free of charge; however, we may impose a 'reasonable fee' to comply with requests for further copies of the same information.
- Where a DSAR has been made electronically, the information will be provided in a secure but commonly used electronic format (e.g. .PDF) unless the data subject requests the information in paper form.
- Under Article 12 of the General Data Protection Regulation, data controllers must respond to a DSAR "without undue delay" and "in any event **within one month of receipt of the request**"
- In the event of numerous or complex requests, the period of compliance can be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.
- Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee can be charged based on the administrative cost of providing the information.
- Where a request is deemed to manifestly unfounded or excessive, in line with the legislation The Caldecott Foundation reserves the right to refuse to respond to the request.
- Any information which is posted must be done so using a registered/recorded postal service.

THE RIGHT TO RECTIFICATION

- Individuals are entitled to have any inaccurate or incomplete personal data rectified.
- Where the personal data in question has been disclosed to third parties, we will inform them of the rectification where possible.
- Where appropriate, The Caldecott Foundation will inform the individual about the third parties that the data has been disclosed to.
- Requests for rectification will be responded to within one month; this can be extended by up to two months where the request for rectification is complex.

Where no action is being taken in response to a request for rectification, The Caldecott Foundation will explain the reason for this to the individual and will inform them of their right to complain to the supervisory authority.

THE RIGHT TO ERASURE

- Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent where consent was the original legal basis for processing the data
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation

The Caldecott Foundation has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- The exercise or defence of legal claims
- As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.
- Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.
- Where personal data has been made public within an online environment, we will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

THE RIGHT TO RESTRICT PROCESSING

- In certain circumstances individual data subjects have the right to block or suppress The Caldecott Foundation's processing of personal data.

The Caldecott Foundation will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until we have verified the accuracy of the data
- Where an individual has objected to the processing and we are considering whether their legitimate grounds override those of the individual
- Where processing is unlawful, and the individual opposes erasure and requests restriction instead
- Where we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim
- If the personal data in question has been disclosed to third parties, we will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.
- We will inform individuals when a restriction on processing has been lifted.

THE RIGHT TO DATA PORTABILITY

Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means, personal data will be provided in a structured, commonly used and machine-readable form.

The Caldecott Foundation will provide the information free of charge.

Where feasible, data will be transmitted directly to another organisation at the request of the individual.

The Caldecott Foundation is not required to adopt or maintain processing systems which are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, we will consider whether providing the information would prejudice the rights of any other individual. Where reasonable we may attempt to obtain permission from other individuals effected or may decide to redact the personal identifiable data for other individuals.

The Caldecott Foundation will respond to any requests for portability within one month.

Where the request is complex, or a number of requests have been received, the timeframe can be extended by up to two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, we will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority.

THE RIGHT TO OBJECT

The Caldecott Foundation will inform individuals of their right to object in its privacy notices.

Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.

The Caldecott Foundation will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the organisation can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- The Caldecott Foundation will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The Caldecott Foundation will not refuse an individual's objection regarding data that is being processed for direct marketing purposes.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, we are not required to comply with an objection to the processing of the data.

PRIVACY BY DESIGN AND PRIVACY IMPACT ASSESSMENTS

The Caldecott Foundation will act in accordance with the UK GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the organisation has considered and integrated data protection into processing activities.

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the organisation's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow the organisation to identify and resolve problems at an early stage, thus reducing risks to the rights and freedoms of data subjects and preventing damage from being caused to The Caldecott Foundation's reputation which might otherwise occur.

A DPIA will be used when introducing new technologies, changing an existing process, undertaking a new project or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

Where appropriate a DPIA may be used for more than one project or process.

High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences

The Caldecott Foundation will ensure that all DPIAs include the following information:

- A description of the nature, context and purpose of the processing
- An assessment of the necessity and proportionality of the processing
- An outline of the risks to data subjects
- The measures implemented in order to address the identified risks

Where a DPIA indicates high risk data processing, we may consult the ICO to seek its opinion as to whether the processing operation complies with the data protection law.

DATA BREACHES

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The management team will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their continuous development training.

All staff, governors and Trustees should be aware of their responsibilities to report any incident that they think may constitute a data breach without delay to Timothy Allison, HR & Business Manager or Jonathan Butler Data Protection & IT Officer as soon as possible.

Where a breach is likely to result in a risk to the rights and freedoms of individuals and is likely to have a significant detrimental effect on the individuals, the relevant supervisory authority will be informed.

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of The Caldecott Foundation becoming aware of it.

The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the organisation will notify those concerned directly.

A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

In extreme cases where a sufficiently serious data breach occurs and where it is not possible to contact the individuals affected by direct means, the organisation may make the details of the data breach public in order that individuals can take their own remedial actions i.e. changing passwords, cancelling credit cards etc.

Effective and robust breach detection, investigation and internal reporting procedures are in place at The Caldecott Foundation, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified. In most cases advice from our DPO would be sought.

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects.

DATA SECURITY

- Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.
- Confidential paper records will not be left unattended or in clear view anywhere with general access.
- Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.
- Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.
- Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted and authorised by The Caldecott Foundation.
- All electronic devices are password-protected to protect the information on the device in case of theft.
- Where possible, The Caldecott Foundation enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- Staff and Trustees will not use their personal laptops or computers for work purposes unless using a method explicitly sanctioned by the organisation.
- All members of staff are provided with their own secure login and password which must meet the organisation's password requirements.
- Emails containing sensitive or confidential information are encrypted if there are unsecure servers between the sender and the recipient.
- Emails to groups of recipients such as parents will be sent blind carbon copy (bcc), so that email addresses are not disclosed to other recipients.
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the organisation's premises accepts full responsibility for the security of the data.

Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of The Caldecott Foundation containing sensitive information are to be supervised at all times.

The physical security of the organisation's buildings and storage systems, and access to them, is reviewed on a regular basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

The Caldecott Foundation takes its duties under the data protection law seriously and any unauthorised disclosure may result in disciplinary action. Where an unauthorised disclosure was intentional or malicious this may be considered Gross Misconduct and may result in dismissal.

The Data Manager is responsible for ensuring that data continuity and recovery measures are in place for the security of protected data.

PUBLICATION OF INFORMATION

The Caldecott Foundation makes only the following information routinely available:

- Policies and procedures

The Caldecott Foundation will not publish any personal information, including photos, on its website without the permission of the affected individual(s).

When uploading information to the organisation's website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

CCTV AND PHOTOGRAPHY

- The Caldecott Foundation understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.
- The Caldecott Foundation will publish a CCTV policy.
- The Caldecott Foundation will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.
- If The Caldecott Foundation wishes to use images/video footage of pupils in a publication, such as the organisation's website, written permission will be sought for the particular usage from the individual with parental responsibility for the pupil and the pupil themselves.
- Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

DATA RETENTION

- Data will not be kept for longer than is necessary.
- Unrequired data will be deleted as soon as practicable.
- Paper documents will be shredded, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

DBS DATA

- All data provided by the DBS will be handled in line with data protection legislation.

- Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data processor.

USE OF SECURE EMAIL SYSTEMS AND NON-SECURE EMAIL SYSTEMS

- The majority of communication with local authorities and social care services is via secure email systems. Where this is not the case, all emails must reference children, colleagues and others related to the business of our organisation, **using initials only**. When using non-secure emails, content must be thought through before the 'send' button is pressed. If there is any potential concern regarding confidentiality or breaching data protection guidance, the email should not be sent.

- All caldecottfoundation.co.uk emails have a disclaimer.

CONFIDENTIALITY

- Employees are required to keep confidential about The Caldecott Foundation's business and that of its children and families both during their employment and at any time after their termination. All information gained in the course of an employee's employment, remains confidential except in circumstances in which they are required to disclose information to a new employer or to a statutory authority. Employees must not remove any documents or tangible items which belong to the organisation or which contain any confidential information from the organisation's premises at any time without due cause. This includes the unauthorised use of any headed paper containing the organisation's logo and/or contact details.

- Employees must return to the organisation if requested and, after consultation, and in any event upon the termination of your employment, all documents and tangible items which belong to The Caldecott Foundation or which contain or refer to any confidential information and which are in their possession or under their control.

- Employees must, if requested by any Manager, and after consultation, delete all confidential information from any re-usable material and destroy all other documents and tangible items which contain or refer to any confidential information and which are in their possession or under their control.

- Employees are not permitted to disclose information reproducing the organisation's passwords or security codes to unauthorised personnel during their employment or at any time after termination of employment. Keys and electronic fobs allocated by the organisation must not be passed on or made available to unauthorised persons within or external to the organisation.

- Employees who have access to the organisation's accounts and financial transactions are not permitted to disclose this information without the authorisation of the Data Manager or a Trustee.

- All employment contracts will include a confidentiality statement or state that the employee must comply with the organisation's data protection policy.

POLICY REVIEW CYCLE

This policy and all policies at The Caldecott Foundation will be reviewed and updated by the management team & Board of Trustees as per our policy review cycle.