Data Protection Policy

Approved on: 4th October 2024

To be reviewed by: October 2027

Signed: Position: Trustee

Signed: Position: Trustee

Introduction

Eagle's Nest Project needs to collect and use certain types of information about young people and other individuals who support or access support from the Charity.

Data Protection Principles

Eagle's Nest Project regard the lawful and correct treatment of personal information as very important and therefore ensure that personal information is treated lawfully and correctly. To this end, Eagle's Nest Project fully endorses and adheres to the Principles of Data Protection, as detailed in the Data Protection Act 1998 ("DPA 98") and article 5 of the General Data Protection Regulation (GDPR). This legislation requires that personal data shall be:

- Processed lawfully, fairly and in a transparent manner;
- 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 are 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; and
- 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.

- **General Provisions**
- This policy applies to all personal data processed by Eagle's Nest Project and includes the personal data of:
- Employees (staff and volunteers)
- Supporters and fundraisers
- Users of our service, their families and the organisations that refer them to us.

- As the Data Controller under the DPA 98 and 2018, Eagle's Nest Project determines for what purposes the personal data it holds will be used. This is outlined on documentation when data is collected. This policy shall be reviewed at least every three years.

- The EAGLE'S NEST PROJECT designated Data Protection Officer (DPO) is Jonathan Horleston-Wilkes (Deputy Head of Centre). He can be emailed at jhw@eaglesnestproject.or.uk or telephoned on 07832199921. The key responsibilities of the DPO are to:
    - Oversee changes to systems and processes;
    - Monitor compliance with the GDPR;
    - Report on data protection and compliance with legislation to trustees;
    - Liaise, if required, with the Information Commissioner's Office (ICO).

- **Lawful, fair and transparent processing**
- Eagle's Nest Project will ensure that data is collected and processed within a lawful, fair and transparent way as per the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form either electronically or in hardcopy.

- When collecting data, Eagle's Nest Project will ensure that the Individual/organisation:

- Clearly understands the purposes for why the information is needed and what it will be used for
- Is made aware of the consequences of deciding not to give consent to processing
- Grants explicit consent for their data to be processed using opt in / opt out selection
- Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
- Will be advised that they can revoke their consent at any time and be advised how to do so.

- **Lawful purposes**
- All data processed by Eagle's Nest Project will be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests. Where consent is relied upon as a lawful basis for processing data, evidence of informed opt-in or other explicit consent shall be kept with the personal data held. Where communications are sent to individuals based on their consent, the option for the individual to unsubscribe will be clearly available.

- **Disclosure**
- Eagle's Nest Project may have to share data with other agencies such as public sector authorities, funding bodies and other voluntary agencies, but will only do so with express consent. The Individual/member will be made aware how and with whom their information will be shared.

- There are circumstances where the law allows Eagle's Nest Project to disclose data (including sensitive data) without the data subject's consent. These include:

- Carrying out a legal duty or as authorised by the Secretary of State
- Protecting vital interests of an Individual/member or other person
- The Individual/member has already made the information public
- Conducting any legal proceedings, obtaining legal advice or defending any legal rights
- Monitoring for equal opportunities purposes – i.e. race, disability or religion
- Providing a confidential service where the Individual/members consent cannot be obtained or where it is reasonable to proceed

Data Minimisation

Eagle's Nest Project shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. They will not hold personal data on the off-chance that it might be useful in the future. This will only happen if it is permissible to hold such information for a foreseeable event that may never occur e.g. contacting a next of kin in the event of an accident.

Data Accuracy

Eagle's Nest Project shall take reasonable steps to ensure that any personal data we obtain is clear and accurate. Eagle's Nest Project will take all reasonable steps to ensure that information provided is kept up to date by asking data subjects whether there have been any changes. Where changes have been made we will ensure systems and records are updated promptly. All individuals, parents and organisations have a responsibility in helping Eagle's Nest Project to keep their data accurate and up to date.

Storage

Eagle's Nest Project will ensure that personal data is only kept for as long as it is needed or required by statute. This is outlined in the privacy statement. Data will be held in as few places as necessary and staff should not create additional duplicating files/folders within cloud storage or on their computer desktop.

Individual & Other Rights

Eagle's Nest Project will adhere to the GDPR rights for individuals which stipulate:

- The ***right to be informed*** about the collection and use of their personal data. Eagle's Nest Project will provide individuals with privacy information including the purposes for processing their personal data, retention periods for that data and who it will be shared with.
- The ***right to access*** their personal data and supplementary information so they can be aware of and verify the lawfulness of the processing. This includes subject access requests (SAR) from the student themselves (if over 13 and/or able to understand the response to the request), those who have parental responsibility or those who have permission to act on behalf of an individual. To submit a SAR the individual should apply in writing (although an application can be made in any format e.g. verbally, by text or email), detailing the information they require access to, this should then be sent to the Data Protection Officer. It is the responsibility of Eagle's Nest Project to treat a request for information as a SAR (e.g. a parent asking for a copy of an incident report is a SAR). In some cases, Eagle's Nest Project may need to ask for proof of identity before processing the request, if this is the case we will inform the individual which documents we require. If proof of identity is not required, Eagle's Nest Project will make a record of why this decision was made. Eagle's Nest Project will respond to a request within one month from the date of receipt and this will normally be in an electronic format, unless requested otherwise. If a subject access request is manifestly unfounded or excessive the organisation is not obliged to comply with it. Alternatively, the organisation can agree to respond but will charge a fee based upon the administrative cost of responding to the request. Eagle's Nest Project will record each SAR using the Compass template- SAR (see appendix 1).
- The ***right to rectification or erasure*** allows individuals to request that any inaccurate personal data is rectified/updated or that their data is permanently erased. A request for rectification or erasure should be made in writing to the Eagle's Nest Project Data Protection Officer (as above) who will complete the request within one month from the date of receipt. Electronically held data will be irretrievably deleted, hardcopy data will be shredded and disposed of securely.
- The ***right to restrict processing*** enables individuals to restrict or stop how their data is being processed whereby it's no longer necessary for the purposes of the processing; if the individual's rights override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data) or if there is a dispute relating to this override of individuals rights.

- The ***right to object*** to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling) and direct marketing (including profiling). Individuals can also complain to the Information Commissioner if they think EAGLE'S NEST PROJECT has failed to comply with data protection legislation.

Data Security
Eagle's Nest Project takes the security of data seriously and has internal controls in place to protect against loss, accidental destruction, misuse or disclosure and to ensure data is not accessed except by employees / volunteers in the undertaking of their duties.

Eagle's Nest Project will ensure that personal data held on computer databases and electronic devices are secured with password protection and encryption protocols. Where personal data is required to be kept in hardcopy format, (e.g. Personnel files), these will be secured in lockable storage.

Transfer
Eagle's Nest Project will ensure that personal information is not transferred outside the European Economic Area (EEA) without reassurance of adequate safeguards being in place from third parties holding this data. Where Eagle's Nest Project are required to share/transfer data to other bodies we shall only do so with the express consent of the data subject. The only instance whereby this would be invalid is if we have to disclose data under the circumstances stipulated in the section titled disclosure above.

Accountability
Eagle's Nest Project take responsibility for complying with the GDPR, at the highest management level and throughout our organisation. We will keep evidence of the steps we take to comply with the GDPR and will put in place appropriate technical and organisational measures to safeguard personal information. This will include:

- Adopting, implementing and reviewing our data protection policy and underpinning policies on a regular basis
- Taking a 'data protection by design and default' approach - to ensure data protection measures are in place throughout the lifecycle of our processing operations;
- Implementing appropriate security measures and recording/reporting personal data breaches;
- Ensuring data protection safeguards are an integral part of our risk assessment processes

Staff Responsibilities & Training
Eagle's Nest Project will provide training on data protection responsibilities to all staff, volunteers and trustees as part of their induction process and yearly refresher training will be provided during staff meetings. In the course of their employed/voluntary role, staff and volunteers may have access to the personal data of others and where this is the case the organisation relies on individuals to help meet its data protection obligations.

Individuals who have access to personal data are required to:

- Understand that they are contractually responsible for adhering to good data protection practice.
- Only access data that they have authority to access and only for authorised purposes.
- Not disclose data except to individuals who have appropriate authorisation whether internal or external to the organisation.
- Keep data secure by complying with the rules on access to premises, computer access, including password protection, secure file storage and ongoing deletion/shredding of documents that are no longer required for the purpose intended.
- Not to remove personal data or portable devices containing or that can be used to access personal data from the organisation's premises without adopting appropriate security measures such as encryption/password protection and not leaving devices unattended or within vehicles.
- Not to store personal data on local drives or on personal devices that are used for work purposes.

A failure to observe these requirements may lead to disciplinary action which will be dealt with under the organisation's disciplinary policy.

Two Key Definitions

Personal Information – Information about living individuals that enables them to be identified – e.g. name, address, online identifiers (IP address). It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers or employees within Eagle's Nest Project.

Sensitive personal data – refers to data about:

- Racial or ethnic origin
- Political affiliations/opinions
- Religious or philosophical beliefs
- Trade union membership
- Physical or mental health
- Sexuality
- Biometric data
- Criminal record or proceedings

Data breach procedure

Definition of an incident

An incident in the context of this policy is an event which has caused or has the potential to cause unauthorised disclosure of and / or damage to Eagle's Nest information or reputation.

<u>Examples of an Information Security Breach are:</u>

• Accidental loss or theft of sensitive or personal data or equipment on which such data is stored (e.g. loss of paper record, laptop, iPad or USB stick)

• Unauthorised or accidental use, access to or modification of data or information systems (e.g. sharing of user login details, deliberately or accidentally, to gain unauthorised access or make unauthorised changes to data or information systems)

• Unauthorised or accidental disclosure of sensitive or personal information (e.g. email sent to an incorrect recipient or document posted to an incorrect address or addressee), or personal data posted onto the website without consent

• Damage or destruction or loss of personal data, or accidental or unlawful alteration of personal data (e.g. due to failure of equipment, or changes or deletions made by staff of documents on shared drives or EN systems)

• Compromised user account (e.g. accidental disclosure of user login details through phishing)

• Failed or successful attempts to gain unauthorised access to EN Information or information systems

• Equipment failure resulting in the non-availability of data

• Malware infection

• Disruption to or denial of IT services

Some of these examples may result in a Personal Data breach. This is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data. While all Personal Data breaches are information security incidents, not all information security incidents are necessarily Personal Data breaches. A Personal Data breach occurs where information relating to identifiable living individuals is involved.

Reporting an incident and record-keeping

It is the responsibility of the discovering member of staff to report information security incidents immediately to the Director, who will determine whether individual data subjects should be informed about the breach. Reports of Personal Data breaches should be sent promptly to the Trustees. Reports should be an accurate description of the incident, including who is reporting the incident, what type of information the incident relates to, and, if Personal Data is involved, how many people it may affect and the category of people (e.g. Staff, Student, etc.). Details should be provided using the Incident Reporting Form (see appendix 2).

Investigation and Risk Assessment

The Director will instigate an appropriate incident investigation within 24 hours of the incident being discovered, where possible. The Chair of Trustees will be notified promptly and will support the investigation, depending on risk management.

The investigation will establish the nature of the incident, the type of data involved, and will consider the extent of a system compromise or the sensitivity of the data. A risk assessment will be performed as to what might be the consequences of the incident, for instance whether data access or IT services could become disrupted or unavailable.

Where Personal Data breaches are concerned, the risk assessment will consider whether there is a risk involved to individuals. This risk assessment will consider the nature, sensitivity and volume of personal data involved, and the number of data subjects; the ease of identification of individuals from the data; the category of data subject, for instance whether they are a child or a vulnerable person; what might be the consequences of the incident and the severity of the impact this would have and the likelihood of this occurring. These factors will help to determine whether there is a risk, or a high risk. The risk assessment will determine whether the incident should be reported to the ICO and whether data subjects should be informed.

Containment and Recovery

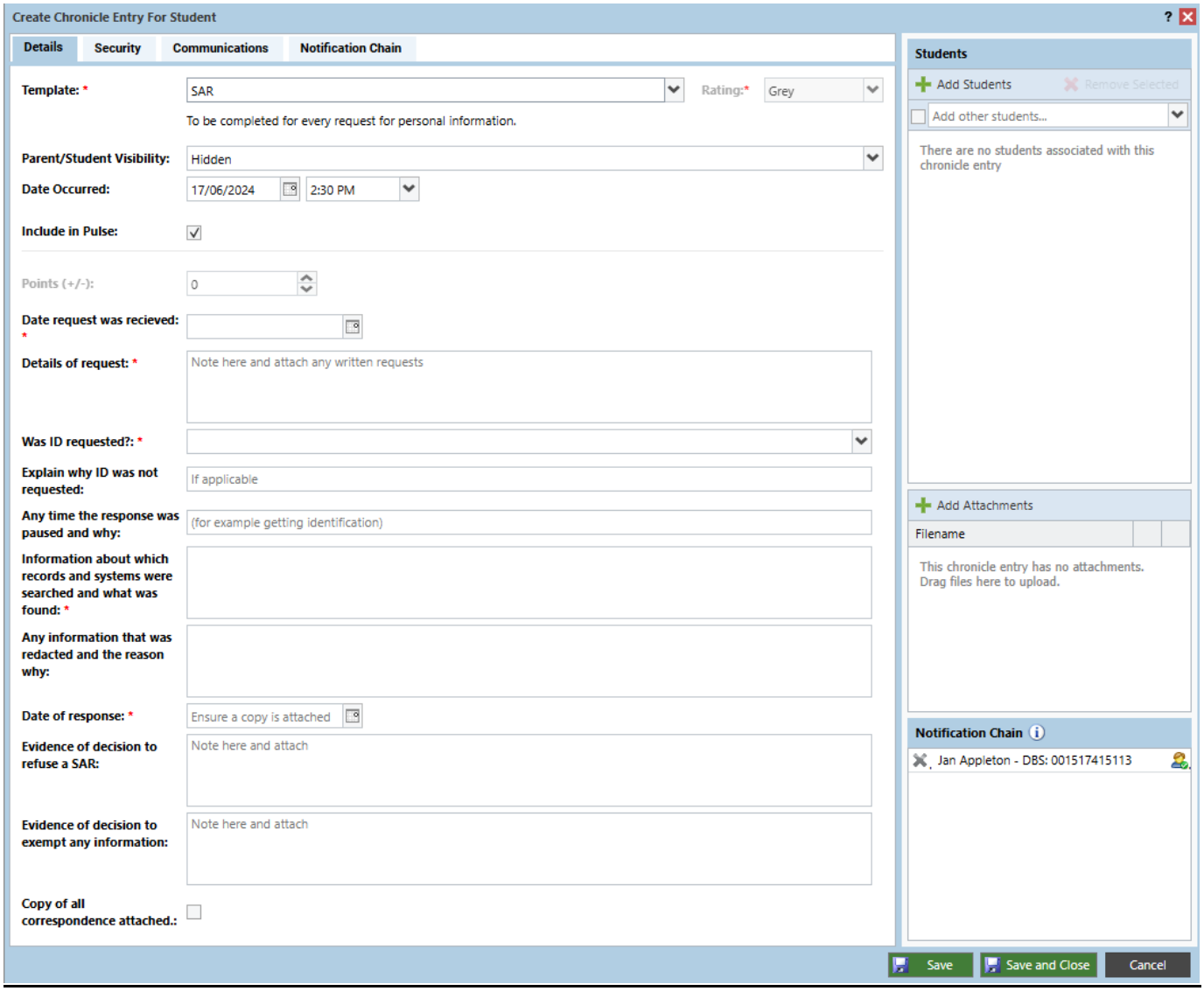
The incident management team, (Director, Chair of Trustees and required technical support), will determine the appropriate course of action and the required resources needed to limit the impact of the incident. This might require isolating a compromised piece of IT equipment, alerting relevant staff.

Appropriate steps will be taken to recover system or data losses and resume normal operation. This might entail attempting to recover any lost equipment, using backup mechanisms to restore compromised or stolen data and changing compromised passwords.

External Notification

The Director and Chair of Trustees will make a decision to inform any external organisation, such as the police or other appropriate regulatory body. If a breach involving Personal Data has occurred, they will inform the Information Commissioner's Office (ICO) if necessary, based on the risk assessment which has been undertaken. If there is considered to be a risk to people’s rights and freedoms (under the General Data Protection Regulation) then the ICO will be informed without undue delay and where feasible not later than 72 hours after Eagle’s Nest has become aware of the breach.

Appendix 1


Create Chronicle Entry For Student
Details
Security
Communications
Notification Chain
Template: *
SAR
Rating:*
Grey
To be completed for every request for personal information.
Parent/Student Visibility:
Hidden
Date Occurred:
17/06/2024
2:30 PM
Include in Pulse:
Points (+/-):
0
Date request was recieved: *
Details of request: *
Note here and attach any written requests
Was ID requested?: *
Explain why ID was not requested:
If applicable
Any time the response was paused and why:
(for example getting identification)
Information about which records and systems were searched and what was found: *
Any information that was redacted and the reason why:
Date of response: *
Ensure a copy is attached
Evidence of decision to refuse a SAR:
Note here and attach
Evidence of decision to exempt any information:
Note here and attach
Copy of all correspondence attached.:
Students
Add Students
Remove Selected
Add other students...
There are no students associated with this chronicle entry
Add Attachments
Filename
This chronicle entry has no attachments.
Drag files here to upload.
Notification Chain
Jan Appleton - DBS: 001517415113
Save
Save and Close
Cancel

Appendix 2

Report of an Information Security Incident or Data Breach

Person reporting the incident				
Date of incident				
Description of incident:				
Is Personal Data involved?	**Yes**		**No**	
Categories of personal data (e.g. name, address, Banner ID, etc.)				
Categories of data subject (e.g. student, staff)				
Number of data subjects involved (if known)				
Any initial action taken in response to incident				