Inclusion Hampshire Policy - General Data Protection Regulation (GDPR)

1. Statement of intent

Inclusion Hampshire is required to keep and process certain information about it's staff members and learners in accordance with it's legal obligations under the General Data protection Regulation (GDPR) and is on the Information Commissioner's Office (ICO) Data protection register.

Inclusion Hampshire (the 'controller') may be required to share information about it's staff or learners with other organisations including but not limited to, schools, Local Authority, educational bodies and Social Services.

This policy is in place to ensure all staff and trustees are aware of their responsibilities and outline how we comply with the following core principles of the GDPR.

2. Legal Framework

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

- The General Data Protection regulation (GDPR)
- The Freedom of Information Act 2000
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004

3. Applicable Data

For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual. The GDPR applies to both electronically stored personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as chronologically ordered data and pseudonymised data, eg key - coded.

Sensitive personal data, known as 'Special categories of personal data' (Article 9 GDPR) processing should be kept extra secure, these include: racial and ethnic origin, political opinions, religious and philosophical beliefs, trade unions, genetic or biometric data, health, sexual life and sexual orientations.

4. 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 are inaccurate, having regards 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; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving for statistical purposes, subject to implementation of the appropriate organisational measures required by GDPR in order to safeguard the rights and freedoms of individuals.
- 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 organisational measures.

The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

5. Accountability

- Inclusion Hampshire will implement appropriate organisational measures to demonstrate that data is processed in line with the principles set out in GDPR
- Inclusion Hampshire will provide comprehensive, clear and transparent privacy policies.
- Special consideration will be given to processing of special category data.
- Internal records of processing activities will include the following:

- Name and details of organisations who process data on our behalf
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of organisational security measures
- Details of transfers to third countries.

Inclusion Hampshire will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation
- Pseudonymisation
- Transparency
- Continuing creating and improving security features.

Data protection impact assessments will be used, where appropriate.

6. Data protection officer (DPO)

A DPO will be appointed in order to:

- Inform and advise Inclusion Hampshire and its employees about their obligations to comply with the GDPR and other data protection laws.

- Monitor Inclusion Hampshires compliance with GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.
The DPO will report to the CEO and Trustee board.
The DPO will operate independently and will not be dismissed or penalised for performing their task. And sufficient resources will be provided to enable them to meet their GDPR obligations.

7. Lawful processing
The legal basis for processing will be identified and documented prior to data being processed.
Under GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained
- For the performance of a contract with the data subject or to take steps to enter into a contract
- Where there is a legal obligation to do so.
- Protecting the vital interests of a data subject or another person (health and wellbeing).
- The performance of a task carried out in the public interest or by, or on behalf of a lawful authority.
- For the purposes of legitimate interests pursued by Inclusion Hampshire or the subject data.

Where personal data is transferred to a country or territory outside the European Economic Area. we will do so in accordance to data protection law.

8. Consent
Inclusion Hampshire understands that 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 unambiguous indication of the individual's wishes.
Where consent is given, a record will be kept documenting how and when consent was given.

Inclusion Hampshire ensures that consent mechanisms meet the standards of GDPR. Where consent is not the most appropriate legal basis, an alternative for processing the data will be used.
Consent accepted under the DPA will be reviewed to ensure it meets the standards of GDPR; however acceptable consent obtained under the DPA will not be re-obtained.

Inclusion Hampshire understands that consent can be withdrawn by the individual at any time.
The consent of parents will be sought prior to the processing of a child's data, except where the processing is related to preventative or counselling services offered directly to a young person.

9. The right to be informed
The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.
If services are offered directly to a young person, Inclusion Hampshire will ensure that the privacy notice is written in a clear, plain manner that they will understand.
In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller (Inclusion Hampshire), and where applicable, the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
  - Withdraw consent at any time.
  - Lodge a complaint with a supervisory authority.

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, this information will be supplied at the time the data is obtained.
In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.

- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

10. The right of access
Individuals have the right to obtain confirmation that their data is being processed.

Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.
Parents / Carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.

Parents also have the right to make a SAR with respect to any personal data held about them.
Inclusion Hampshire will verify the identity of the person making the request before any information is supplied.

If a SAR is made and we do hold information on the individual we will:

- Give a description of what we hold
- Explain why we are holding and processing it, and how long we will keep it for
- Say who it has been, or will be shared with
- Inform if any automated decision-making is being applied to the data, and any consequences of this

A copy of the information will be supplied to the individual free of charge; however, Inclusion Hampshire may impose a 'reasonable fee' to comply with requests for further copies of the same information or is manifestly unfounded or excessive. Any fees will be based on the administrative cost of providing the information.
Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.
All requests will be responded to without delay and at the latest, within one month of receipt.

11. The right to rectification (Article 17 GDPR)
Individuals are entitled to have any inaccurate or incomplete personal data rectified without delay.
Where the personal data in question has been disclosed to third parties, Inclusion hampshire will inform them of the rectification where possible.
Where appropriate, Inclusion Hampshire will inform the individual about the third parties that the data has been disclosed to.

12. The right to be forgotten. (Article 16 GDPR)

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
- 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
- Where instructed to do so by a joint controller of data.

13. The right to restrict processing (Article 18 GDPR)
Individuals have the right to restrict Inclusion Hampshire processing their personal data.
In the event that processing is restricted, Inclusion Hampshire will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.
As directed in Article 18 of GDPR, Inclusion Hampshire 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 Inclusion Hampshire has verified the accuracy of the data
- Where processing is unlawful
- Where Inclusion Hampshire no longer needs the personal data for the purpose collected.
- Where an individual has objected to the processing and Inclusion Hampshire is considering whether their legitimate grounds override those of the individual

If the personal data in question has been disclosed to third parties, Inclusion Hampshire will inform them about the restriction on the processing of the personal data.

14. The right to data portability (Article 20 GDPR)
Individuals have the right to obtain and reuse their personal data for their own purposes across different services.
Data subjects have the the right to be given their data in a structured and commonly used machine readable format and ask for it to be sent to another organisation of their choice.

15. The right to object
Inclusion Hampshire will inform all individuals of their right to object, this will be in the privacy notice and presented clearly and separately from any other information.

16. Data protection impact assessments
Inclusion Hampshire will act in accordance with the GDPR by adopting a Data protection by design approach which demonstrates how it 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 Inclusion Hampshire's data protection obligations and meeting individuals' expectations of privacy.
A DPIA will be used as part of the planning or when reviewing organisational processes or activities, especially in the use of special category data, they will include:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose (by data flow mapping)
- An outline of the risks to individuals

- The measures implemented in order to address risk

17. Data breaches

The term 'personal data breach' refers to a breach of security which has led to the accidental or unlawful destruction, loss, alteration, disclosure or access to personal data transmitted, stored or otherwise processed.
The CEO will ensure that all staff members are made aware of, and understand, what constitutes as a data breach as part of their continuous development training.
Effective and robust breach detection, investigation and internal reporting procedures are in place at Inclusion Hampshire, which facilitate decision-making in relation to whether the Information Commissioner's Office (ICO) need be informed or the relevant data subjects only .
Within a breach notification, the following information will be outlined (Article 34 GDPR):

- The nature of the personal data breach, including the categories and approximate number of data subjects and details 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

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the Information Commissioner's Office (ICO) will be informed. All notifiable breaches will be reported to the ICO within 72 hours of Inclusion Hampshire becoming aware of it. The risk of the breach having a detrimental effect on the individual, and the need to notify the ICO , will be assessed on a case-by-case basis, if not required to be reported to the ICO it must be detailed on the internal breach log.

18. 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 and stored on the Inclusion Suite cloud based system only accessible by authorised persons via individual logins.

Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

All electronic devices are password-protected to protect the information on the device in case of theft.

When staff use personal or external agency laptops or computers to access Inclusion Suite cloud based system, they must not download any documents containing identifiable data.

All necessary members of staff are provided with their own secure login and password to Inclusion Suite and are encouraged to change their password regularly plus log out of all systems when not using.

Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

Emails to multiple persons outside of the organisation are sent blind carbon copy (bcc), so 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 Inclusion Hampshire 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.
- Who will receive the data has been outlined in a privacy notice.

Under no circumstances are visitors allowed access to confidential or personal information.

Visitors to Inclusion Hampshire are supervised at all times to ensure they have no access to data. The physical security of Inclusion Hampshire's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

Inclusion Hampshire takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

The Data Protection Officer is responsible for continuity and recovery measures are in place to ensure the security of protected data.

19. Data retention

Data will not be kept for longer than is necessary, and only ever in line with referring schools and agencies and the current guidelines for that specific purpose.

Unrequired data will be deleted as soon as practicable.

Paper documents will be shredded and electronic memories deleted, once the data should no longer be retained.

20. DBS data

All data provided by the DBS will be handled in line with data protection legislation and the regulatory umbrella organisation we use to process them. Information relating to the completion of and details of the disclosure will be only available to the CEO (and any Senior Managers as they deem necessary) and the HR Officer for Inclusion Hampshire.

Data Protection Officer: Emma Barnard

Contact: info@inclusionhampshire.org.uk

POLICY IMPLEMENTATION

The Chief Executive is responsible for ensuring the implementation of this policy and that regular reviews take place.

The DSL is responsible for ensuring updates pertaining to safeguarding are passed to the Chief Executive to be written into this policy.

All staff have a responsibility to adhere to this policy and will be made aware of this policy as part of their induction, supervision and on-going training.

Failure for staff to act in line with this policy will result in disciplinary action.