Data Protection Policy

(Version 2 : Revised 26 Jun 23)

Adopted by The Hawksmoor Learning Trust	Signature	
	Print Name	
	Date	
	On behalf of the Hawksmoor Learning Trust	

Contents

Introduction

1. The Trust is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller, the handling of such data in line with the;
   1.1 data protection principles (see below) and
   1.2 Data Protection Act (DPA) 2018.
2. Changes to data protection legislation (General Data Protection Regulations May 2018) will be monitored and implemented to remain compliant with all requirements:
3. **Article 6 Lawfulness of processing**
   3.1 Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller;
4. **Article 9 Processing of special categories of personal data.**
   4.1 Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
   4.2 Paragraph 3 shall not apply if one of the following applies. The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to above may not be lifted by the data subject.
   4.3 The requirements of this policy are mandatory for;
      4.3.a. all staff employed by The Hawksmoor Learning Trust (THLT) and
      4.3.b. any third party contracted to provide services.
   4.4 If personal information meets the above criteria, then individuals who have personal information held by THLT will be made aware of the personal information and the criteria for holding the information in the 'Information Audit' document, held in the Trust Office.

Roles

5. **Data Controller.**
   5.1 The member of staff responsible for data protection in each school, the Data Controller, is shown in appendix 1.
   5.2 The Data Controller may delegate data controller duties as necessary.
   5.3 The Data Controller is the person who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any personal data is to be processed.

6. **Data Protection Officer (DPO).**

6.1 The Data Protection Officer (DPR) is a named employee of Plumsun; details are at Annex A

6.2 The DPO;

6.2.a. monitors internal compliance,

6.2.b. informs and advises the trust / school about their data protection obligations and

6.2.c. acts as a contact point for data subjects and the supervisory authority.

6.3 The DPO is;

6.3.a. independent,

6.3.b. an expert in data protection,

6.3.c. adequately resourced and

6.3.d. reports to the highest management level ie the Trust Board.

7. All staff must;

7.1 treat all student information in a confidential manner and

7.2 follow the guidelines as set out in this document.

8. Any Data Processors, processing data on behalf of the school (ie external organisations) must;

8.1 confirm that they are achieving their obligations under the UK General Data Protection Regulation (GDPR) and

8.2 are registered with the Information Commissioner's Office (ICO).

9. Roles under GDPR can be found on the ICO Website

Training.

10. The Trust / school is committed to ensuring that staff are aware of data protection policies and legal requirements.

Notification.

11. Data processing activities and persons responsible will be registered with the Information Commissioner's Office (ICO) as required by the ICO. Details are available from the ICO: https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

12. Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

13. Breaches of personal or sensitive data will be notified to the;

13.1 individual(s) concerned and

13.2 ICO as specified in the GDPR Regulations.

Personal and Sensitive Data.

14. All data within the Trust's / school's control shall be identified as personal, sensitive or both to ensure that;

    14.1 it is handled in compliance with legal requirements and

    14.2 access to it does not breach the rights of the individuals to whom it relates.

15. The definitions of personal and sensitive data shall be those published by the ICO for guidance.

Principles.

16. Under the GDPR, the data protection principles are set out the main responsibilities for organisations.

17. **Article 5 of the GDPR requires that personal data shall be;**

    17.1 'processed lawfully, fairly and in a transparent manner in relation to individuals;

    17.2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

    17.3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

    17.4 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;

    17.5 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 purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

    17.6 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.'

18. Article 5(2) requires that:

    18.1 'the controller shall be responsible for, and be able to demonstrate, compliance with the principles.'

19. Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.

The need for consent.

20. The Trust / school will ask for consent to hold and process personal information if there is no lawful basis for doing so (see article 6 and Article 9 above).

Data Breaches.

21. All data breaches must be immediately reported to the relevant Data Controller identified in Annex A.

22. The Data Protection Controller will assess whether the breach needs to be reported to the ICO and / or individuals concerned.

23. The Data Controller will;

    23.1 make any necessary reports and

    23.2 take immediate action to;

        23.2.a. review how the breach has occurred and

        23.2.b. make any necessary changes to procedures to ensure that the same problems do not arise in the future.

24. The DPO will;

    24.1 provide a monitoring role and

    24.2 be a contact point for the supervisory authority as necessary.

Protection Impact Statements.

25. The Trust / school will evidence the thought and decision-making process about data protection when designing any processes in school which involve personal data.

26. A Data Protection Impact Statement (DPIA) is needed when:

    26.1 new technology is being deployed,

    26.2 a profiling operation is likely to significantly affect individuals,

    26.3 there is processing on a large scale of the special categories of data ('special categories' as specified in GDPR guidance)

Individuals Rights:

27. Individuals have the right to;

    27.1 be informed about what data is being held (Information Audit Document held by the Trust),

    27.2 be informed about how and why the data is being processed (Information Audit Document held by the Trust),

    27.3 the right to;

        27.3.a. access any data that is being held (see Subject Access Requests below),

        27.3.b. request that any data is erased (see Subject Access Requests below),

        27.3.c. restrict processing,

27.3.d. data portability (that the individual can transport the data held about them to another service) if the data is held by automatic means and

27.3.e. object to the way data is being held or processed.

27.4 The right not to be subject to automated decision-making.

27.5 The individual can write to the Data Controller regarding requests;

27.5.a. for data to be erased,

27.5.b. to restrict processing,

27.5.c. to data portability,

27.5.d. to not be subject to automated decision-making or

27.5.e. the right to object to the way data is being held or processed.

Biometric Data:

28. As well as adhering to GDPR regulations in respect to sensitive data, the Trust / school will also adhere to DfE Guidance 'Protection of biometric information of children in schools and colleges' March 2018. This section is referred to as the school's statutory biometric policy.

29. The school;

29.1 will treat the data collected with appropriate care and

29.2 must comply with the data protection principles as set out in the GDPR.

30. Where the data is used as part of an automated biometric recognition system, the school will comply with the additional requirements in sections 26 to 28 of the Protection of Freedoms Act 2012.

31. The school will ensure that each parent of a child is notified of the school's intention to use the child's biometric data as part of an automated biometric recognition system.

32. The written consent of at least one parent will be obtained before the data is taken from the child and used. This applies to all pupils under the age of 18. In no circumstances will a child's biometric data be processed without written consent.

33. The school will not process the biometric data of a pupil (under 18 years of age) where:

33.1 the child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data,

33.2 no parent has consented in writing to the processing or

33.3 a parent has objected in writing to such processing, even if another parent has given written consent.

34. The school must provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system.

35. The biometric information will only be held as long as it is relevant to do so.

36. Biometric information is included the school's information audit, which is publicly available.

Sharing of Information with Third Parties:

37. There may be circumstances where the school is required either by law or in the best interests of students or staff, to pass information onto external authorities, eg local authorities, Ofsted or the department of health. These authorities are required to;
    - 37.1 adhere to data protection law and
    - 37.2 have their own policies relating to the protection of any data that they receive or collect.
38. Personal data about children, will not be disclosed to third parties without the consent of the;
    - 38.1 child (at an age who can act for themselves, specified under GDPR guidance) or
    - 38.2 the child's parent or carer, unless it is obliged by law or in the best interest of the child.
39. Examples of data that may be disclosed to third parties without the need for consent may include;
    - 39.1 other schools if a pupil transfers from one school to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school.
    - 39.2 examination authorities eg for registration purposes, to allow the pupils at the school to sit examinations set by external exam bodies.
    - 39.3 health authorities (under health legislation), the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.
    - 39.4 police and courts if a situation arises where a criminal investigation is being carried out, THLT / school may have to forward information on to the police to aid their investigation.
    - 39.5 social workers and support agencies to protect or maintain the welfare of pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.
    - 39.6 Department for Education (DfE) and Ofsted to help the government monitor and audit school performance and enforce laws relating to education.
40. The intention to share data relating to individuals to an organisation outside of the school will be clearly defined within notifications and details of the basis for sharing given. These details are provided in the 'Information Audit Document' held at the Trust Office.
41. Data will be shared with external parties in circumstances where it is;
    - 41.1 a legal requirement to provide such information or
    - 41.2 for the purpose of pupil provision, such as school meals and on-line curriculum work.
42. Any proposed change to the processing of individual's data will be notified to the individual.
43. Under no circumstances will the Trust / school disclose information or data;
    - 43.1 that would cause serious harm to the child or anyone else's physical or mental health or

condition,

43.2 indicating that the child is or has been subject to child abuse or may be at risk of it,

43.3 where the disclosure ***would not*** be in the best interests of the child,

43.4 that would allow another person to be identified or identifies another person as the source, unless;

43.4.a. the person is an employee of the Trust / school or a local authority or

43.4.a.i has given consent or

43.4.a.ii it is reasonable in the circumstances to disclose the information without consent.

43.5 The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed.

Data Access Requests (Subject Access Requests).

44. All individuals, whose data is held by the Trust / school, have a legal right to request access to such data or information.

45. A child may make a subject access request for themselves, specified under GDPR guidance.

46. The school shall respond to such requests within one month.

47. All requests must be made in writing to the Data Controller, who may delegate the request.

48. In line with THLT / school safeguarding and GDPR obligations, some personal information may be redacted for reasons such as;

48.1 information that might cause serious harm to the physical or mental health of the pupil or another person or

48.2 information containing personal information about more than one individual.

49. The DPO will;

49.1 advise, independently, any requests as necessary and

49.2 act as a contact point for data subjects and the supervisory authority.

50. No charge will be applied to process the request.

51. There is a right to appeal to the ICO upon dispute of a decision.

Right to be Forgotten:

52. Where any personal data is no longer required for its original purpose, an individual can demand that;

52.1 the processing is stopped and

52.2 all their personal data is erased by the Trust / school including any data held by contracted processors.

Photographs and Video.

53. Images of staff and pupils may be captured;

53.1 at appropriate times and

53.2 as part of educational activities for use in Trust / school only.

54. Unless prior consent from parents / pupils / staff has been given, the Trust / school must not utilise such images for publication or communication to external sources.

55. It is the Trust's / school's policy that external parties (including parents) may not capture images of staff or pupils during such activities without prior written consent.

Location of Information and Data.

56. Hard Copy.

56.1 Hard copy data, records, and personal information are stored out of sight and in a locked filing cabinets. The only exception to this is medical information, attendance registers and signing in books (which must be immediately accessible and used in the case of an emergency).

56.2 Sensitive or personal information and data should not be removed from the Trust / school site. It is accepted that some staff may need to transport data between the Trust / school and their home to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings or are on school visits with pupils.

56.3 Risks of identified breaches from existing processes have been;

56.3.a. considered and

56.3.b. recorded on an Impact Assessment Form.

56.4 The following guidelines are in place for staff to reduce the risk of personal data being compromised;

56.4.a. paper copies of data or personal information should not be taken off the Trust / school site, unless the Data Controller has provided written permission to do so (such as the need for emergency information during educational visits). If there is no other way to avoid taking a paper copy of data off the Trust / school site, the information must not be;

56.4.a.i on view in public places or

56.4.a.ii left unattended under any circumstances,

56.4.b. unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name,

56.4.c. care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers,

56.5 Soft Copy.

56.5.a. For the purposes of this policy, PC includes any mobile electronic device

capable of storing and amending data eg smart phones, tablets etc.

56.5.b. The preferred method personal data storage is cloud-based using Teams.

56.5.c. Access to personal data will be closely controlled through selective access to the relevant Team.

56.5.d. No member of staff must give access to any Team containing personal data without the authority of the FD.

56.5.e. If personal data is downloaded from the cloud to a PC for amendment;

56.5.e.i it must be uploaded back to the cloud when no longer needed and

56.5.e.ii the downloaded copy must be deleted when no longer required.

56.5.f. No personal data is to be stored on personal IT devices.

56.5.g. If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended; sensitive information should not be viewed on public computers.

56.5.h. If it is necessary to transport data away from the Trust / school, it should be downloaded onto a password protected USB stick or computer. Computers will also be encrypted if it viable to do so.

56.5.i. Personal data should not be transferred from computers or USB onto any public computers. Work should be edited from the USB and saved onto the USB or authorised computers only.

57. These guidelines will be clearly communicated to all school staff.

58. Any person who is found to be intentionally breaching, or has breached, this conduct may be subject to discipline in line with the seriousness of their misconduct.

Personal Data Taken Off Site

59. Only employees of the Trust may take sensitive data off site.

60. Sensitive data must only be taken off site when absolutely necessary and never routinely.

61. Sensitive data downloaded from Teams must be uploaded to Teams once the work has been completed and copies stored to local drives deleted immediately.

62. It is the responsibility of the employee removing the sensitive data off-site to ensure it is protected and stored in line with this policy.

63. It is the responsibility of the employee removing the sensitive data downloaded from Teams to ensure it is protected and stored in line with this policy.

64. Failure to protect and store data in a compliant manner may become a disciplinary matter.

65. In the case of a breach or potential breach, the employee accessing or using sensitive data off-site must report any this to the Data Controller identified in Annex A immediately on discovering the breach.

Data Security.

66. To assure the protection of all data being processed and inform decisions on processing activities, the Trust / school will undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them.

67. Risk and impact assessments will be conducted in;

    67.1 accordance with guidance given by the ICO and

    67.2 compliance with the GDPR.

68. Security of data will be achieved through the implementation of proportionate physical and technical measures.

69. Nominated staff will be responsible for;

    69.1 the effectiveness of the controls implemented and

    69.2 reporting of their performance.

70. The security arrangements of any organisation with which data is shared will be considered and, where required, these organisations will be required to provide evidence of the competence in the security of shared data.

Data Disposal.

71. The Trust / school recognises that the secure disposal of redundant data is an;

    71.1 integral element to compliance with legal requirements and

    71.2 area of increased risk.

72. All data held in any form of media (paper, tape, electronic) will only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

73. All data will be destroyed or eradicated to agreed levels, meeting recognised national standards, with confirmation at completion of the disposal process.

74. Disposal of IT assets holding data will be disposed of in compliance with ICO guidance.

Annex A. Roles

1. **Data Controllers.**

1.1	BLPS	The Head Teacher
1.2	NHPS	The Executive Principal
1.3	MWPS	The Executive Principal
1.4	TRPS	The Executive Principal
1.5	Central Trust	The Executive Principal

2. **Data Protection Officer (DPO).** Ruth Hawker, Plumsun Ltd. Contact details.

2.1 **Info@Plumsum.**com

2.2 **Tel:** 074 5862 2684