POPPY HILL
CHURCH OF ENGLAND MULTI ACADEMY TRUST

Data Protection Policy

Date to be reviewed	December 2023
Policy Status	Statutory
Responsible member	Mrs K Evans

This policy applies to all schools and stakeholders within Poppy Hill Academy Trust

General Data Protection Regulation

Our Commitment:

Henlow Church of England Academy is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and the Data Protection Act (DPA).

https://ico.org.uk/for-organisations/guide-to-data-protection/data-protectionprinciples/

Changes to data protection legislation (GDPR May 2018) shall be monitored and implemented in order to remain compliant with all requirements.

The legal bases for processing data are as follows –

a) Consent: the member of staff/student/parent has given clear consent for the school to process their personal data for a specific purpose.

b) Contract: the processing is necessary for the member of staff's employment contract or student placement contract.

c) Legal obligation: the processing is necessary for the school to comply with the law (not including contractual obligations)

The members of staff responsible for data protection are the Business Administrator, Deputy Head Teacher and ICT Technician. However, all staff must treat all student information in a confidential manner and follow the guidelines as set out in this document.

The school is also committed to ensuring that its staff members are aware of data protection policies, legal requirements and adequate training is provided to them through online training via Luton Council.

The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

Notification:

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

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

Breaches of personal or sensitive data shall be notified within 72 hours to the individual(s) concerned and the ICO.

Personal and Sensitive Data:

All data within the school's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

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

https://ico.org.uk/for-organisations/guide-to-data-protection/keydefinitions/

The principles of the Data Protection Act shall be applied to all data processed:

- ensure that data is fairly and lawfully processed
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive
- ensure that data processed is accurate
- not keep data longer than is necessary
- process the data in accordance with the data subject's rights
- ensure that data is secure
- ensure that data is not transferred to other countries without adequate protection.

Fair Processing / Privacy Notice:

We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and pupils prior to the processing of individual's data.

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.

https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-noticestransparency-and- control/

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities, for example

local authorities, Ofsted, or the department of health. These authorities are up to date with data protection law and have their own policies relating to the data protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of our school shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

Any proposed change to the processing of an individual's data shall first be notified to them. Under no circumstances will the school disclose information or data:

- that would cause serious harm to the child or anyone else's physical or mental health or condition
- indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child
- recorded by the pupil in an examination
- that would allow another person to be identified or identifies another person as the source, unless the person is an employee of the school or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed
- in the form of a reference given to another school or any other place of education and training, the child's potential employer, or any national body concerned with student admissions.

Data Security:

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall 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.

Risk and impact assessments shall be conducted in accordance with guidance given by the ICO:

https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/
https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2014/02/privacyimpact- assessments-code-published/

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.

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

Data Access Requests (Subject Access Requests):

All individuals, whose data is held by us, have a legal right to request access to such data or information about what is held. We shall respond to such requests within twenty working days.

Requests should be made in writing to:

GDPR Administrator

Poppy Hill Church of England Multi Academy trust

Church Road

Henlow

Bedfordshire

SG16 6AN

No charge will be applied to process the request.

The Trust can refuse to comply with a SAR if it is:

- manifestly unfounded; or
- manifestly excessive.

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. Data may be disclosed to the following third parties without consent:

- Other schools If a pupil transfers from Henlow Church of England Academy to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as

is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.

- Examination authorities;
    - This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.
- Health authorities
    - As obliged 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.
- Police and courts
    - If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.
- Social workers and support agencies
    - In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.
- Educational Division
    - Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.
- Right to be Forgotten
    - Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the school including any data held by contracted processors.

Photographs and Video:

Using images of children for publicity purposes will require the age appropriate consent of the individual concerned and their legal guardians. Images should not be displayed on websites, in publications or in a public place without such consent. The definition of a

public place includes areas where visitors to the school have access. The school collects consent from parents/guardians and this should be checked prior to utilising photographs in this way.

Biometric Recognition Systems

Biometric data means personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can be their fingerprint, facial shape, retina and iris patterns, and hand measurements.

Where Poppy Hill Academy Trust uses pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash or library book loans), the school/entity will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The schools will get written consent from at least one parent or carer before taking any biometric data from their child and first process it (this applies to all pupils/students in settings under the age of 18).

Parents/carers and pupils have the right to choose not to use the biometric system(s). The school will provide alternative means of accessing the relevant services for those pupils.

Parents/carers and pupils can withdraw consent, at any time, and the school will make sure that any relevant data already captured is either deleted or undergoes a process of irreversible anonymisation. As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, the school will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the biometric system(s), the school will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object.

Staff and other adults can also withdraw consent at any time, and the school will either delete any relevant data already captured or ensure it undergoes a process of irreversible anonymisation. Poppy Hill Academy Trust will ensure that biometric data is stored securely to prevent any unauthorised or unlawful use. Biometric data will only be used for the purposes for which it has been obtained.

Location of information and data:

Hard copy data, records, and personal information are stored out of sight and in a locked cupboard. The only exception to this is medical information that may require immediate access during the school day. This will be stored with the school medical coordinator.

Sensitive or personal information and data should not be removed from the school site, however the school acknowledges that some staff may need to transport data between the school and their home in order 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.

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

- Paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.
- 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.
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
- 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.
- If it is necessary to transport data away from the school, it should be uploaded into google drive to be accessed from other locations/devices.

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

Data Disposal:

The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

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

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

Disposal of IT assets holding data shall be in compliance with ICO guidance:

https://ico.org.uk/media/fororganisations/documents/1570/it_asset_disposal_for_organisations.pdf

The school has identified a qualified source for disposal of IT assets and collections. The school also uses Shred-Station to dispose of sensitive data that is no longer required.

The schools Data Protection officer is Ms Paula Creighton, STP Compliance Ltd.

The school's internal GDPR Lead is Mrs K Evans.