



Data Protection Policy

Watchorn Christian School 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) will be implemented and subsequent amendments monitored in order to remain compliant with all requirements.

The legal bases for processing data are–

- (a) **Consent:** the member of staff/child/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 or child's funding contract.
- (c) **Legal obligation:** the processing is necessary for the school to comply with the law (not including contractual obligations)

The personnel at the school responsible for data protection are the head teacher and governors.

However, all staff must treat all student information in a confidential manner and follow the guidelines set out in this document. The school is also committed to ensuring that its staff are aware of data protection policies and legal requirements.

Personal and Sensitive Data:

All data within the school's control will 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 will 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 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 will 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-notice/transparent-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 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.

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.../data-protection-impact-assessments>

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

Data Access Requests (Subject Access Requests):

All individuals whose data is held by us, has a legal right to request access to such data or information about what is held. We shall respond to such requests (having sought advice regarding sensitive information within one month and they should be made in writing using the schools Access Request Form to:

Mrs C Pearson,

Watchorn Christian School

Alfreton

Derbys

DE55 7 AQ

No charge will be applied to process the request.

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 Watchorn School 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. 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 all their personal data is erased by the school

Photographs and Video:

Images of staff and pupils may be captured at appropriate times for many different reasons and as part of educational activities for use in and by school only. Unless prior consent from parents/pupils/staff has been given, the school shall not utilise such images for publication or communication to external sources. It is the school's policy that external parties (including parents) may not capture images of staff or pupils during such activities without prior consent. Photographs to be used in marketing type material will have specific informed consent, and only be used in line with the consent provided.

Location of information and data:

Hard copy data, records, and personal information are stored out of sight and in a locked filing cabinet.

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:

- Staff should avoid taking paper copies of data off the school site. If there is no way to avoid taking a paper copy of data off the school site, (e.g. school visits) 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.
- If at all possible download data onto a USB stick. The data should not be transferred from this stick onto any home or public computers. Work should be edited from the USB and saved onto the USB only.
- 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 Retention

Please refer to our Data Retention Schedule for information as to how long a piece of information should be kept.

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 or 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.

Personal Data Breaches

A breach of data which is likely to result in an individual suffering damage will be reported e.g. breaches that could result in identity theft or where an individual's confidentiality has been breached. However, at Watchorn School any breach in data security will be investigated by the DPO (Mrs Pearson and the governing body). It will also be recorded on an internal breach register.

Where the school detects a breach which is subject to the mandatory reporting rules it will report the breach to the supervisory group without delay and not later than 72 hours after becoming aware of it. Where a breach has to be reported to affected individuals this will be done without undue delay.

Protection of biometric information of children in schools

At present we do not use or store any biometric information of children at our school.

Reviewed 08/07/2020