Kendrick School
Confidentiality Policy

Approval Date: July 2024

Next Review Date: July 2026

Version: CP- V1 2018	
Version: CP-V2 2020	
Version: CP-V3 2022	
Version: CP- V4 2024	

Kendrick School
Confidentiality Policy

This policy must be read in conjunction with Kendrick School's Inclusion Policy and Safeguarding Policy and in compliance with Data Protection Law 2018 which incorporates General Data Protection Regulations.

Aim
To ensure that all members of staff working on the school site are clear about levels of confidentiality that they must offer to the school community and can expect themselves. Confidentiality is a whole school issue. All staff must be clear about the boundaries of their legal and professional roles and responsibilities and that no member of staff can offer or guarantee absolute confidentiality due to safeguarding issues. This policy ensures good practice throughout the school which is understood by parents/carers. It also aims to protect children and young people at all times and to give the school workforce clear, unambiguous guidance as to their legal and professional roles in relation to sharing information and confidentiality, ensuring good practice throughout the school.

Background
Kendrick School's Confidentiality Policy conforms to the law, government guidance and recommendations.

Rationale
Kendrick School fosters an ethos of mutual respect and trust and sensitivity to the needs of others. The right to privacy for all members of the school community must be respected. All personal matters must be discussed discreetly for the protection of individuals concerned and a consistent approach when handling information about students and staff must be observed. Ground rules are set (see below), and a safe environment is created where a whole variety of issues and topics can be discussed openly in the learning and teaching environment where no personal questions will be asked.

Kendrick School undertakes a school information and impact assessment audit to ensure all electronic and hard copy information of personal records are held in compliance of the new regulations, integrated into the GDPR principles and held securely. Staff will receive training; IT procedures will be reviewed and policies reviewed.

Definitions:
Information about staff may be information held electronically or in hard copy. Personal information may also be disclosed to line managers or others verbally on a need-to-know basis. See **Code of Conduct Policy and the Data Protection Act.** New Staff Privacy Notices details the information held, how it may be used and processed and the access rights of staff to their information and their right to object.

Information about students may be held electronically or in hard copy. Personal Information may also be disclosed to members of staff on a need-to-know basis. This information may be about themselves, their family, parents/carers, friends or others. New Student Privacy Notices available for parents and students will detail the information held, how it may be used and processed and the access rights of students over the age of 12 years and their parents/carers to their information and their right to object.

PERSONAL DATA

'Personal data' is information that identifies an individual, and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain[1]. A sub-set of personal data is known as 'special category personal data'. This special category data is information that reveals:

race or ethnic origin;
political opinions;

religious or philosophical beliefs;
trade union membership;
physical or mental health;
an individual's sex life or sexual orientation;
genetic or biometric data for the purpose of uniquely identifying a natural person.

Special Category Data is given special protection, and additional safeguards apply if this information is to be collected and used.

Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

Kendrick School does not intend to seek or hold Special Category Data (previously known as sensitive personal data) about staff or students except where the school has been notified of the information, or it comes to the school's attention via legitimate means (e.g., a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice. Staff or students are under no obligation to disclose to the school their race or ethnic origin, political or religious beliefs, whether or not they are a trade union member or details of their sexual orientation (save to the extent that details of marital status and / or parenthood are needed for other purposes, e.g., pension entitlements).

The Data Protection Principles

The six data protection principles as laid down in the GDPR are followed at all times:

- personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met;

- Personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;

- personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed;
- personal data shall be accurate and, where necessary, kept up to date;
- personal data processed for any purpose(s) shall not be kept in a form which permits identification of individuals for longer than is necessary for that purpose / those purposes;

- personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

Disclosure of personal information outside the school will only be made with the informed consent of the individuals concerned, except:

- to assist in the detection or prevention of a criminal offence (e.g., the police, Inland Revenue) or comply with a court order, or a reasonable request from a relevant statutory body (Children's Social Care, CAFCASS,)
- where there is a clear child protection concern, health or safety risk or evidence of fraud;
- in connection with court proceedings or statutory action;
- anonymously for bona fida statistical or research purposes, provided it is not possible to identify the individuals to whom the information relates.

Context regarding confidentiality when dealing with students

- Staff will generally have access to all information that they genuinely need to know to carry out their work, and are under a duty to respect the confidentiality of all personal information held by the school.
- Information about individual students regarding performance, progress and attainment will be shared only with their own parents/carers. Parents/carers must not have access to any information about other students (who are not their own child or of whom they are not carers) at any time.
- Where a student seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or carers, the school will maintain confidentiality unless it has reasonable grounds to believe that the student does not fully understand the consequences of withholding their consent, or where the school believes disclosure will be in the best interests of the student or other students. Disclosure for a safeguarding purpose will be lawful due to the substantial public interest raised.
- All confidential information about students will be kept securely and/or encrypted.
- Personal or confidential information about students and staff will not normally be taken off school premises. Those authorised to do this (Headteacher, Deputy Headteacher and SLT) **must** keep such information securely and/or encrypted.
- Child protection records will be kept separately and will only be accessible by the school's Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Leads.
- Addresses and telephone numbers of parents and students will not be passed on except in exceptional circumstances or to a receiving school. (e.g., to the Local Authority for child protection purposes, Evolve as data processors for adventurous school trips).
- Where individual students are discussed in school (e.g., in behaviour support or Trustees' Disciplinary meetings), any reports or paperwork will be marked as confidential and kept securely.
- Confidential information from a student may be passed on to appropriate members of staff **when the student is considered to be at risk.** In such cases a member of staff has a legal, moral and contractual obligation to pass on that information to the DSL in order to safeguard the welfare of the student. (See safeguarding policy if in any doubt.)
- Students are made aware of the school's policy, by tutors or specialist PSHCE staff by giving regular reminders at the start of PHSCE courses, usually at the beginning of the school year or when specific topics are to be addressed. Students have to be clearly informed of the school's position.
- Only in the most exceptional circumstances will the school be in a position of having to handle information without parental knowledge. This will be on the grounds for serious concern and where child protection issues should be addressed. Parents of Sixth Form students above the age of 16 will only be contacted following discussions with the students as necessary.
- Photographs of students should not be used without parents/carers permission and at no time should the student's name be used with a photograph so they can be individually identified.

Information disclosures and the law

If a student shares sensitive or personal information to a member of staff that is not of a child protection nature or a criminal offence, the position of the member of staff is that she or he does not have to break the confidence of the student. If the information however gives cause for the member of staff to believe that the student is at risk of harm or a criminal offence has been, or is about to be, committed against the student, or by the student, then the member of staff **must** pass on that information to the Designated Safeguarding Lead (DSL). At Kendrick all staff are advised to share information with the permission of the student (other than child protection issues or criminal offences) with a senior member of staff or the Headteacher, however teachers are not legally bound to inform parents or the Headteacher of any disclosure unless the Headteacher has specifically requested them to do so. In matters of child protection or criminal offences the Headteacher will then take the necessary course of action deemed to be in the best interests of the student.

Procedure following a disclosure of information

Other than in child protection cases or criminal offences, when a student shares any personal or sensitive information with a member of staff, the member of staff concerned must in the first instance stay calm and reassure the student that the seriousness of the situation has been appreciated and that as a result of the information a certain course of action may have to be considered. The member of staff must explain that the information may have to be passed on, in the first instance to the Pastoral Leaders who will then arrange a meeting with their Line Manager. The student's anonymity may be preserved throughout this process depending on the nature of the information/disclosure. The meeting between the members of staff concerned will then consider the course of action required and which professionals need to be involved. The course of action taken will be based on the individual situation, the professional judgement of the members of staff concerned and the best interests of the student. The position of the parents' role and responsibilities will be discussed and one of the members of staff may discuss this with the student to try to encourage the student to confide in her parents. **Information about a student may only be shared if consent is given by the student and parents and only on a need-to-know basis except in some child protection matters.**

Summary of action following information/disclosure:
Member of staff ➔ Pastoral Leader/ Deputy DSL ➔ DSL➔ Headteacher

In all child protection concerns, the DSL, as designated person for child protection, or the Headteacher, in their absence, **must** be informed without delay, as delay may be prejudicial to the welfare of the student.

Confidentiality of the process
Throughout the process brief details will be recorded and kept securely in a separate file to the student's file. **Under no circumstances will the individual student's identity or details be discussed or shared with any other member of staff in the school outside the pastoral group concerned.**

Health Professionals to consult/other possible avenues for support
Within the school the student has access to:

1. **The School Nurse.** Individual appointments are available and a weekly drop-in session is also held.

2. **No. 5 Counselling Service.** No 5 offers a confidential counselling service to individual students. Any student is allowed to visit the counselling service without parental knowledge (subject to Gillick competence), via individual appointments

There is a wide range of outside agencies that a student or member of staff can access for advice or support. Personal information about the student should not be disclosed to these agencies without prior discussion with the Headteacher or Deputy Headteacher or DDSLs. These include the following:

- NSPCC
- The Source (Reading – Drug and Alcohol)
- The Samaritans
- Family Planning Association
- Department of Sexual Health (RBH)
- Rape Crisis Line

Subject Access Requests

Anybody who makes a request to see any personal information held about them by the School is making a subject access request. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure, provided that they constitute a "filing system".

The individual's full subject access right is to know;

- whether personal data about him or her are being processed

- the purposes of the processing
- the categories of personal data concerned
- the recipients or categories of recipient to whom their personal data have been or will be disclosed
- the envisaged period for which the data will be stored or where that is not possible, the criteria used to determine how long the data are stored
- the existence of a right to request rectification or erasure of personal data or restriction of processing or to object to the processing
- the right to lodge a complaint with the Information Commissioner's Office
- Where the personal data are not collected from the individual, any available information as to their source
- Details of the safeguards in place for any transfers of their data to locations outside the European Economic Area.

All requests should be sent to the Headteacher within 3 working days of receipt, and must be dealt with in full without delay and at the latest within one month of receipt, subject to various exemptions.

Where a child or young person does not have sufficient understanding to make his or her own request (usually those under the age of 12, or over 12 but with a special educational need which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. The Headteacher working in collaboration with the GDPR Lead in school, must however be satisfied that:

- the child or young person lacks sufficient understanding; and
- the request made on behalf of the child or young person is in their interests.

Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances the school must have written evidence that the individual has authorised the person to make the application and the Headteacher must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

A subject access request must be made in writing. The school may ask for any further information reasonably required to locate the information.

An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

All files must be reviewed by the GDPR Lead before any disclosure takes place. Access will not be granted before this review has taken place.

Where all the data in a document cannot be disclosed a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

Exemptions to access by data subjects

Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived.

There are other exemptions from the right of subject access. If we intend to apply any of them to a request then we will usually explain which exemption is being applied and why.

Breach of GDPR Compliance

Any and all breaches of the GDPR, including a breach of any of the data protection principles shall be reported as soon as it is discovered, to the Headteacher, the GDPR Lead (SBM) or another member of the SLT.

Once notified, the Headteacher or GDPR Lead shall assess:

- the extent of the breach;
- the risks to the data subjects as a consequence of the breach;
- any security measures in place that will protect the information;
- any measures that can be taken immediately to mitigate the risk to the individuals.

Unless the Headteacher or GDPR Lead concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the school, unless a delay can be justified.

The Information Commissioner shall be told:

- details of the breach, including the volume of data at risk, and the number and categories of data subjects;
- the contact point for any enquiries (which shall usually be the GDPR Lead
- the likely consequences of the breach;
- measures proposed or already taken to address the breach.

If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the Headteacher working with the GDPR Lead, shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

Data subjects shall be told:

- the nature of the breach;
- who to contact with any questions;
- measures taken to mitigate any risks.

The Headteacher or GDPR Lead shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the SLT and Governing Body and a decision made about implementation of those recommendations.

Visitors

The school's confidentiality policy applies to relevant visitors to the school (e.g., school nurse, those conducting PHSCE sessions) who will be consulted about this either in advance of the visit or when they come to school. Visitors are expected to comply with the policy and meet with the Headteacher on arrival.

Monitoring and review
The Senior Leadership Team at the start of the school year and in the light of any new recommendations from government, will regularly review the policy.

Ownership and reference to other policies
Trustees have agreed the policy.

Access
The policy statement will be kept on Sharepoint. The policy will be available for all visitors to read.

Reference to other related policies

The policy supports and complements other related policies including, RSE,, Drugs Education, Freedom of Information Policy and Data Protection policy, Child Protection and Safeguarding and Social and Moral Education policies.