בס"ד

CONFIDENTIALITY POLICY

Who is this policy for?	All nursery and school staff, admin staff, therapists and volunteers
Date of this review:	December 2022
Date of next review:	December 2024
Who is responsible for monitoring and evaluating this policy?	Headteacher
Signed of Date: Governing Body	December 2022

ETHOS

Our fundamental belief is that as a school, we are aware that we are placed in a position of trust by all stakeholders and there is an expectation that we will take a professional approach to all matters involving confidentiality. Sharing information unnecessarily is an erosion of that trust.
It is also underpinned by our commitment to keep the Halochos of Loshon Hora and other Torah based ethics.

AIMS

- To protect the children at all times
- To provide consistent messages in school about handling information about children
- To give all staff involved clear, unambiguous guidance as to their legal and professional roles.
- To ensure good practice throughout the school which is understood by pupils, parents and staff.
- To ensure that parents have a right of request access to any records the school may hold on their child (and that there are certain legal restrictions) but not to any other child they do not have parental responsibility for.
- To foster an ethos of trust within the school.

GENERAL GUIDELINES

- All information about individual children is private and should only be shared with staff that need to know.
- All social services, medical and personal information about a child will be held in a safe and secure place which cannot be accessed by individuals other than designated school staff.
- The school prides itself on good communication with parents, carers and staff are always available to talk to both children and parent/carers about issues causing concern.

- Parents/Carers and children need to be aware that the school cannot guarantee total confidentiality and the school has a duty to report child protection issues.
- All children have a right to the same level of confidentiality irrespective of gender, race, religion, medical concerns and educational issues.
- Staff should be aware of children with medical needs and the class information sheet should be accessible to staff who need that information but not on general view to other parents/children.
- On the school website, photographs of children will not include their individual names having had parental consent for the photographs to be used.
- Parents should not have access to any other child's books, teacher comments, reports and progress grades at any time.
- Anyone staff member using the internet, particularly social networking sites e.g Facebook, should ensure that any reference to school or the children would be viewed as warranting disciplinary action.
- Parents should be aware that information about their child will be shared with the receiving school when they change schools.
- Addresses, contact numbers and e-mail address details will not be passed on except in exceptional circumstances (where the school has a legal requirement for the child's safety) or to a receiving school.
- In a close-knit Heimishe community where pupils and their families are known outside school to staff members and other pupils, information that is shared in school must not be shared with any other person outside school, for any reason, without the express permission of a line manager. In a situation where disclosure would be necessary it is essential that halachic guidelines are followed as to what and how much we may disclose 'Letoelles'
- Staff will not share partisan views and opinions in school.

Schools and the Data Protection Act (1998) & UK General Data Protection Regulation (UK GDPR)

If you handle and store information about identifiable, living people, you are legally obliged to protect that information. As such you must:

- Only collect information you need for a specific purpose
- Keep it secure
- Ensure it is relevant and up to date
- Only hold as much as you need, for as long as you need it
- Allow the subject of the information to see it on request

The school is registered with the ICO and renewed annually.

PART ONE: PUPIL INFORMATION

Access to pupil information

Under the Data Protection Act a pupil has the right to a copy of information held about them. If a child is too young or unable to make that request themselves, parents have a right to ask on their behalf. The Education (Pupil Information) (England) Regulations 2005 also state that a parent has the right to access their child's educational record.

This record includes information held on computer, information held in files, unstructured information, for example, loose correspondence, and any other information held in any format. A pupil is also entitled to be told what information is held by the school, the purposes it is used for, and who it is released to.

If parents request information that may involve the details of other pupils being disclosed, that request will be considered carefully on its own merits.

The school is exempt from disclosing information in the following circumstances:

- The information may cause serious harm to the physical or mental health of the pupil or another individual
- Cases where disclosure would reveal a child is at risk of abuse
- Information contained in adoption and parental order records
- Information given to a course in proceedings under the Magistrate's Courts (Children and Young Person) Rules 1992
- Copies of examination scripts
- Providing examination marks before they are officially announced

All requests for information must come in writing from the parents to the Head teacher. Requests should be met within 15 days unless exceptional circumstances apply, and these will be communicated to parents. A fee may be charged to parents if excessive copying of material is required. Fees will be charged in accordance with the scale suggested by the Information Commissioner's Office, and can be accessed at www.ico.gov.uk.

Confidentiality of pupils and pupil records and information

Disclosures

- School staff should never promise confidentiality. Pupils do not have the right to expect they will not be reported to their parents, and no member staff should give a promise that assures confidentiality
- All teachers, therapists and health professionals receive safeguarding training and in the event of a disclosure, they should follow the school's safeguarding policy and procedures
- We expect all non-teaching staff to report any disclosures by parents or pupils of a concerning nature to the designated child protection coordinator as soon as possible after the disclosure in an appropriate setting, so that others cannot

overhear. The designated child protection officer will decide what, if any further action needs to be taken

- Staff may need support when dealing with personal information and issues concerning pupils. We prefer staff to ask for help from their line manager in these cases (and therefore share information) rather than making poor choices about what to do with any information disclosed. Staff should not take worries about pupils home with them

Sharing pupil information verbally & protecting pupils' written records

- We believe that all staff should be able to share their concerns about pupil safety and well being, but it is important to be aware that personal information is sensitive. Concerns should be shared with the staff member's immediate line manager, who will then make a decision about who to share this information with, if anyone
- General conversations about pupil family circumstances, sensitive personal information and other factors affecting the life of that child and their family should not take place unless there is a sound educational reason to share this information
- Written records should always be kept securely. Staff should challenge any unknown person who appears to be accessing pupil written records
- Written records must not leave the school premises unless in exceptional circumstances and without the express permission of the Head teacher
- Electronic devices such as laptops and member sticks that may contain pupil information must be kept securely

Taking photographs of children in school

- Photos taken for personal use by parents of their children in school are exempt from the Data Protection Act.

Other photos taken by the school are subject to the Data Protection Act, and so the following good practice should apply:

- Children and parents should be aware when photos/film is being taken that may be shared outside the school – e.g. for prospectus' or for local newspapers
- Permission must be gained from parents before photos of their children are shared
- Where many children are photographed, for example, during a school awards ceremony or a whole school activity, permission need not be sought, as long as parents are aware that photos may be taken and used beforehand

PART TWO: STAFF INFORMATION

The Data Protection Act covers information held about staff in a similar way as it covers information held about pupils. It ensures the school regulates the way that information held about staff is used, and it also gives staff access to information held about them.

Recruitment and Selection

- Information about potential employees will be kept securely.
- Information about potential employees will not be gathered covertly.
- If information gathered in the course of recruitment is to be used for any other purpose, this will be made clear to applicants on the application form
- All employees who handle candidate information will be required to deal with it securely and with respect. It will not be widely circulated
- Only information relevant to the position being advertised will be collected - personal information such as marital status or other unnecessary information will not be gathered
- Information about criminal convictions will be collected, as well as 'spent' convictions under the Exceptions Order of the Rehabilitation of Offenders Act 1974. DBS information will be kept securely
- Applicants will be made aware through our Safe Recruiting Policy that information about them will be checked and verified
- Information obtained through a recruitment exercise will only be kept as long as there is a clear business need for it

Employment Records

- Employment records will be kept about all staff, and they will be kept informed as to how they are used
- Access to these records will be limited to authorised members of staff only
- Anyone who has access to these records will be made aware that they need to be treated with respect
- Information that is irrelevant, excessive or out of date will not be kept
- If any requests are made to disclose information about an employee, the identity of the person making the request will be carefully checked
- Employment records, whether on paper or on computer will be stored securely. Sickness records and other sensitive information will be kept separately to the general employment files. The school may ask about an employee's health to ensure that it can monitor health and safety provision, but an employee is not obliged to answer these questions
- If information is collected to monitor the school's equal opportunities practice, for example, about an employee's disabilities or race, this information will be used for that purpose only
- If there is no longer a sound business need to keep an employee's record, it will be shredded

The rights of employees to request information

- All employees have the right to request information that is held about them. All requests for disclosure must be met by the school within 40 days. This includes information about grievance and disciplinary issues. Consideration will be given when disclosing information where information about another employee would be implicated
- Employees have the right to see information stored about them relating to issues like appraisal. Minutes of these meetings will be shared in advance, and employees will have the right to amend if necessary, or note their disagreement in such cases
- Employees have a right to request copies of references supplied about them
- If the school receives a reference about an employee from a third party that is marked 'in confidence' the school will consider whether the information held is actually confidential, if a request for disclosure is made. Factual information that the employee would already know can reasonably be disclosed. Where a reference may include a previous employers opinions, the referee must be contacted, and their permission sought
- If the referee refuses consent, it may still be justifiable to release the reference. The following factors will be considered:
    - Any express assurance of confidentiality given to the referee
    - Any relevant reasons the referee gives for withholding consent
    - The potential or actual effect of the reference on the individual
    - The fact that a reference must be truthful and accurate and without access to it the individual is not in a position to challenge its accuracy
    - That good employment practice suggests that an employee should already have been advised of any weakness
    - Any risk to the referee

PART THREE: INFORMATION SHARING BETWEEN PROFESSIONALS AND HOW THIS IS AFFECTED BY CONFIDENTIALITY

Information sharing is key to ensuring that all services surrounding children co-ordinate effectively and that safeguarding and early intervention needs are met. This can sometimes conflict with the demands of safeguarding private information about children and families, and so it is important that staff know when and how to share information in an appropriate manner.

There are circumstances when it is appropriate to share information about children with other professionals. For our purposes, it is best practice to share information when:

- We are supporting transitions – between different school phases, or to facilitate integration
- When there are concerns about significant harm to a child
- When there are concerns about significant harm to third parties

Key rules for information sharing are summarised below:

1. The Data Protection Act is not a barrier to sharing information, but provides a framework to ensure that information is shared appropriately
2. Be open and honest with families about what, why, how, when and with whom information will be shared, and seek agreement, unless it is unsafe to do so
3. Seek advice if you are in any doubt about disclosing identities
4. When appropriate and possible, always gain consent for sharing information, but professionals should still share information without consent if they feel that a child is in danger of being harmed if information is withheld
5. Base information sharing decisions on consideration of the safety and well being of the person concerned and others who may be affected by their actions
6. Information shared should be necessary proportionate, relevant, accurate, timely and secure
7. Keep a record of your decision to share information and the reasons for it. If you decide to share information, record what you have shared, with whom and for what purpose

Further information to support a decision to share information are listed below:

- Is there a clear and legitimate purpose for you to share the information?
- Does the information enable a living person to be identified?
- Is the information confidential, and if so, do you have consent to share?
- If consent is refused, do you have good reason not to seek consent and is there sufficient public interest to share the information?
- If the decision is to share, are you sharing information appropriately and securely?
- Are you properly recording your information sharing decision?

If you have any concerns at all about whether it is appropriate to share information about a child, please do not carry these worries alone, but ask the advice of your line manager who will be able to guide you or will seek further legal advice.

Information Off-site

Personal information can only be taken off-site with express permission from the Head teacher or senior member of staff. It remains the responsibility of that person to ensure the records are kept safe and if kept at home over night a designated and locked store is used/

Personal emails (e.g. gmail accounts) are not secure and personal information should not be sent. If you work off-site you should request a SBS email address which offers greater security. Report written from home should only use initials and completed when you come into work.

Information stored or sent electronically should have a password. USB sticks should not be used for personal information unless a password **and** encryption is used (standard USB sticks are not encrypted)

LINKS TO OTHER POLICIES

This policy links to other policies including safeguarding, safer recruitment, and emergency procedures policies.