53. CONFIDENTIALITY AND CLIENT ACCESS TO RECORDS

Policy statement

'Share with informed consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, there is good reason to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case.'

Information sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers (HMG 2023)

It is our intention to respect the privacy of children and their parents/carers, while ensuring that they access high quality early years care and education at ASK. We aim to ensure that all parents/carers can share their information in the confidence that it will only be used to enhance the welfare of their children. We have record keeping systems in place that meet legal requirements; the means that we use to store and share that information takes place within the framework of the General Data Protection Regulations (2018) and the Human Rights Act (1998).

Confidentiality procedures

Most things that happen between the family, the child, and ASK are confidential to ASK. In certain circumstances information is shared, for example, a child protection concern will be shared with other professionals including social care or the police, and settings will give information to children's social workers who undertake S17 or S47 investigations. Normally parents/carers should give informed consent before information is shared, but in some instances, such as if this may place a child at risk, or a serious offence may have been committed, parental consent should not be sought before information is shared. Hounslow Safeguarding Children's Partnership (LSP) procedures should be followed when making referrals, and advice sought if there is a lack of clarity about whether parental consent is needed before making a referral due to safeguarding concerns.

- We keep all records securely (see our Children's Records policy and our Privacy Notice).
- Information is kept in a manual file and/or electronically.
- Electronic copies are held securely on encrypted servers to which only the Registered Provider/owner and setting manager have access.
- We always check whether parents/carers regard the information they share with us to be confidential or not.
- Some parents/carers may share information about themselves with other parents/carers as well as with our members of staff; ASK cannot be held responsible if those parents/carers whom the person has 'confided' in share information.

- Information shared between parents/carers in a discussion or training group is usually bound by a shared agreement that the information is confidential to the group and not discussed outside of it. We are not responsible should that confidentiality be breached by participants.
- We inform parents/carers when we need to record confidential information beyond the general personal information we keep (see our Children's Records policy and our Privacy Notice) - for example with regard to any injuries, concerns, or changes in relation to the child or the family, any discussions with parents/carers on sensitive matters, any records we are obliged to keep regarding action taken in respect of child protection, and any contact and correspondence with external agencies in relation to their child.
- Staff discuss children's general progress and well-being together in meetings, but more sensitive information is restricted to our Registered Provider/Owner, our manager, and the child's key person, and is shared with other members of staff on a need-to-know basis.
- Members of staff do not discuss children with staff who are not involved in the child's care, nor with other parents/carers or anyone else outside ASK, unless in a formal and lawful way.
- Discussions with other professionals should take place within a professional framework, not on an informal basis. Staff should expect that information shared with other professionals will be shared in some form with parent/carers and other professionals, unless there is a formalised agreement to the contrary, i.e. if a referral is made to children's social care, the identity of the referring agency and some of the details of the referral is likely to be shared with the parent/carer by children's social care.
- It is important that members of staff explain to parent/carers that sometimes it is necessary to write things down in their child's file and explain the reasons why.
- When recording general information, staff should ensure that records are dated correctly, and the time is included where necessary and signed.
- Welfare/child protection concerns are recorded on a safeguarding incident reporting form. Information is clear and unambiguous (fact, not opinion), although it may include the educator's thoughts on the impact on the child.
- Records are non-judgemental and do not reflect any biased or discriminatory attitude.
- Not everything needs to be recorded, but significant events, discussions and telephone conversations must be recorded at the time that they take place.
- Recording should be proportionate and necessary.
- When deciding what is relevant, the things that cause concern are recorded as well as action taken to deal with the concern. The appropriate recording format is filed within the child's file.

- Information shared with other agencies is done in line with these procedures and our Information Sharing policy.
- Where a decision is made to share information (or not), reasons are recorded.
- Staff may use a computer to type reports, or letters. Where this is the case, the typed document is deleted from the computer and only the hard copy is kept.
- The setting is registered with the Information Commissioner's Office (ICO). Staff are expected to follow guidelines issued by the ICO, at https://ico.org.uk/for-organisations/guidance-index/
- Additional guidance in relation to information sharing about adults is given by the Social Care Institute for Excellence, at www.scie.org.uk/safeguarding/adults/practice/sharing-information
- Staff should follow guidance including Working Together to Safeguard Children (DfE 2023); Information Sharing: Advice for Practitioners Providing Safeguarding Services to Children, Young People, Parents and Carers 2024 and What to do if you're Worried a Child is Being Abused (HMG 2015)
- Where third parties share information about an individual to us our practitioners and managers check if it is confidential, both in terms of the party sharing the information and of the person whom the information concerns.

Confidentiality definition

- Personal information of a private or sensitive nature, which is not already lawfully in the public domain or readily available from another public source, and has been shared in a relationship, where the person giving the information could reasonably expect it would not be shared with others.
- Staff can be said to have a 'confidential relationship' with families. Some families share information about themselves readily; members of staff need to check whether parents/carers regard this information as confidential or not.
- Parents/carers sometimes share information about themselves with other parents/carers as well as staff; the setting cannot be held responsible if information is shared beyond those parents/carers whom the person has confided in.
- Information shared between parents/carers in a group is usually bound by a shared agreement that the information is confidential and not discussed outside. The setting manager is not responsible should that confidentiality be breached by participants.
- Where third parties share information about an individual; staff need to check if it is confidential, both in terms of the party sharing the information and of the person whom the information concerns.

- Information shared is confidential to the setting.
- Educators ensure that parents/carers understand that information given confidentially will be shared appropriately within the setting (for instance with a designated person, during supervision) and should not agree to withhold information from the designated person or their line manager.

Breach of confidentiality

- A breach of confidentiality occurs when confidential information is not authorised by the person who provided it, or to whom it relates, without lawful reason to share.
- The impact is that it may put the person in danger, cause embarrassment or pain.
- It is not a breach of confidentiality if information was provided on the basis that it would be shared with relevant people or organisations with lawful reason, such as to safeguard an individual at risk or in the public interest, or where there was consent to the sharing.
- The procedure for Children's Records must be followed.

Exception

- GDPR enables information to be shared lawfully within a legal framework. The Data Protection Act 2018 balances the right of the person about whom the data is stored with the possible need to share information about them.
- The Data Protection Act 2018 contains "safeguarding of children and individuals at risk" as a processing condition enabling "special category personal data" to be processed and to be shared. This allows educators to share without consent if it is not possible to gain consent, if consent cannot reasonably be gained, or if gaining consent would place a child at risk.
- Confidential information may be shared without authorisation - either from the person who provided it or to whom it relates, if it is in the public interest and it is not possible or reasonable to gain consent or if gaining consent would place a child or other person at risk. The Data Protection Act 2018 enables data to be shared to safeguard children and individuals at risk. Information may be shared to prevent a crime from being committed or to prevent harm to a child, Information can be shared without consent in the public interest if it is necessary to protect someone from harm, prevent or detect a crime, apprehend an offender, comply with a Court order or other legal obligation or in certain other circumstances where there is sufficient public interest.
- Sharing confidential information without consent is done only in circumstances where consideration is given to balancing the needs of the individual with the need to share information about them.

- When deciding if public interest should override a duty of confidence, consider the following:
  - is the intended disclosure appropriate to the relevant aim?
  - what is the vulnerability of those at risk?
  - is there another equally effective means of achieving the same aim?
  - is sharing necessary to prevent/detect crime and uphold the rights and freedoms of others?
  - is the disclosure necessary to protect other vulnerable people?

The decision to share information should not be made as an individual, but with the backing of the Designated Safeguarding Lead who can provide support, and sometimes ensure protection, through appropriate structures and procedures.

Obtaining consent

Consent to share information is not always needed. However, it remains best practice to engage with people to try to get their agreement to share where it is appropriate and safe to do so.

Using consent as the lawful basis to store information is only valid if the person is fully informed and competent to give consent and they have given consent of their own free will, and without coercion from others, Individuals have the right to withdraw consent at any time.

You should not seek consent to disclose personal information in circumstances where:

- someone has been hurt and information needs to be shared quickly to help them
- obtaining consent would put someone at risk of increased harm
- obtaining consent would prejudice a criminal investigation or prevent a person being questioned or caught for a crime they may have committed
- the information must be disclosed regardless of whether consent is given, for example if a Court order or other legal obligation requires disclosure

NB. The serious crimes indicated are those that may harm a child or adult; reporting confidential information about crimes such as theft or benefit fraud are not in this remit.

- Settings are not obliged to report suspected benefit fraud or tax evasion committed by clients, however, they are obliged to tell the truth if asked by an investigator.
- Parents/carers who confide that they are working while claiming should be informed of this and should be encouraged to check their entitlements to benefits, as it may be beneficial to them to declare earnings and not put themselves at risk of prosecution.

Consent

- Parents/carers share information about themselves and their families. They have a right to know that any information they share will be regarded as confidential as outlined in Privacy notice. They should also be informed about the circumstances, and reasons for the setting being under obligation to share information.
- Parents/carers are advised that their informed consent will be sought in most cases, as well as the circumstances when consent may not be sought, or their refusal to give consent overridden.
- Where there are concerns about whether to gain parental consent before sharing information, for example when making a Channel or Prevent referral, the setting manager must inform their line manager for clarification before speaking to parents/carers.
- Consent must be informed – that is the person giving consent needs to understand why information will be shared, what will be shared, who will see information, the purpose of sharing it and the implications for them of sharing that information.

Separated parents/carers

- Consent to share need only be sought from one parent/carer. Where parents/carers are separated, this would normally be the parent/carer with whom the child resides.
- Where there is a dispute, this needs to be considered carefully.
- Where the child is looked after, the local authority, as 'corporate parent' may also need to be consulted before information is shared.

Client access to records procedures

Under the General Data Protection Regulations there are additional rights granted to data subjects which must be protected by ASK.

The parent is the 'subject' of the file in the case where a child is too young to give 'informed consent' and has a right to see information that ASK has compiled on them.

- If a parent/carer wishes to see the file, a written request is made, which the setting acknowledges in writing, informing the parent/carer that an arrangement will be made for him/her to see the file contents, subject to third party consent.
- Information must be provided within 30 days of receipt of request. If the request for information is not clear, the manager must receive legal guidance, for instance, from Law-Call for members of the Early Years Alliance. In some instances, it may be necessary to allow extra time in excess to the 30 days to respond to the request. An explanation must be given to the parent/carer where this is the case. The maximum extension time is 2 months.

- A fee may be charged to the parent/carer for additional requests for the same material, or any requests that will incur excessive administration costs.
- The setting manager informs the Registered Provider/Owner and legal advice is sought.
- The setting manager goes through the file and ensures all documents are filed correctly, entries are in date order, and that there are no missing pages. They note any information, entry, or correspondence, or other document which mentions a third party. The setting manager should always ensure that recording is of good quality, accurate, fair, balanced, and proportionate, and should have quality assurance processes in place to ensure that files are checked for quality regularly and that any issues are addressed promptly.
- Each of those individuals are written to explaining that the subject of the file has requested sight of the file which contains a reference to them, stating what this is.
- They are asked to reply in writing to the setting manager giving or refusing consent for disclosure of that material.
- Copies of these letters and their replies are kept on the child's file.
- Agencies will normally refuse consent to share information, and the parent should be redirected to those agencies for a request to see their file held by that agency.
- Entries where you have contacted another agency may remain, for example, a request for permission from social care to leave in an entry where the parent was already party to that information.
- Members of staff should also be written to, but the setting reserves the right under the legislation to override a refusal for consent or just delete the name and not the information.
  - If the member of staff has provided information that could be considered 'sensitive,' and the staff member may be in danger if that information is disclosed, then the refusal may be granted.
  - If that information is the basis of a police investigation, then refusal should also be granted.
  - If the information is not sensitive, then it is not in the setting's interest to withhold that information from a parent. It is a requirement of the job that if a member of staff has a concern about a child and this is recorded; the parents/carers are told this at the start and in most cases, concerns that have been recorded will have been discussed already, so there should be no surprises.
  - The member of staff's name can be removed from an entry, but the parent/carer may recognise the writing or otherwise identify who had provided that information. In the interest

of openness and transparency, the setting manager may consider overriding the refusal for consent.

  - In each case this should be discussed with members of staff and decisions recorded.

- When the consent/refusals have been received, the setting manager takes a photocopy of the whole file. On the copy file the document not to be disclosed is removed (e.g. a case conference report) or notes pertaining to that individual in the contact pages blanked out using a thick marker pen.
- The copy file is then checked, and legal advisors verify that the file has been prepared appropriately, for instance, in certain circumstances redaction may be appropriate, for instance if a child may be damaged by their data being seen by their parent/carer, e.g. if they have disclosed abuse. This must be clarified with the legal adviser.
- The 'cleaned' copy is then photocopied again and collated for the parent to see.
- The setting manager informs the parent/carer that the file is now ready and invites him/her to make an appointment to view it.
- The setting manager and the Registered Provider/Owner meet with the parent/carer to go through the file, explaining the process as well as what the content records about the child and the work that has been done. Only the persons with parental responsibility can attend that meeting, or the parent's/carer's legal representative or interpreter.
- The parent/carer may take a copy of the prepared file, but it is never handed over without discussion.
- It is an offence to remove material that is controversial or to rewrite records to make them more acceptable. If recording procedures and guidelines have been followed, the material should reflect an accurate and non-judgemental account of the work done with the family.
- If a parent/carer feels aggrieved about any entry in the file, or the resulting outcome, then the parent/carer should be referred to our Complaints procedure for parents/carers and service users.
- The law requires that information held must be accurate, and if a parent/carer says the information held is inaccurate then the parent/carer has a right to request it to be changed. However, this only pertains to factual inaccuracies. Where the disputed entry is a matter of opinion, professional judgement, or represents a different view of the matter than that held by the parent/carer, the setting retains the right not to change the entry but can record the parent's/carer's view. In most cases, a parent/carer would have had the opportunity at the time to state their side of the matter, and this should have been recorded there and then.

- If there are any controversial aspects of the content of a client's file, legal advice must be sought. This might be where there is a court case between parents/carers or where social care or the police may be considering legal action, or where a case has already completed, and an appeal process is underway.
- A setting should never 'under-record' for fear of the parent/carer seeing, nor should they make 'personal notes' elsewhere.

All the undertakings above are subject to the paramount commitment of ASK, which is to the safety and well-being of the child. Please see also our policy on Safeguarding Children and Child Protection.

Legal framework

- General Data Protection Regulations (GDPR) (2018)
- Human Rights Act (1998)

Further guidance

The Information Commissioner's Office https://ico.org.uk/ or helpline 0303 123 1113.

Working Together to Safeguard Children (DfE 2023)

Information Sharing: Advice for Practitioners Providing Safeguarding Services to Children, Young People, Parents and Carers (HMG 2023)

What to do if you're Worried a Child is Being Abused (HMG 2015)

Mental Capacity Act 2005 Code of Practice (Office of the Public Guardian 2007)

This policy was adopted by:	ASK Kindergarten & Clubs
On:	May 18, 2026
Date to be reviewed:	May 18, 2027
Signatory:	Mark Stewart
Role of Signatory:	Owner & Ofsted Registered Provider