The Stacey Pre-School
Play • Explore • Discover • Learn

15. Confidentiality & Information Sharing Policy

1. Policy statement

The Stacey Pre-School recognises that children, families, employees, volunteers and other individuals have a right to expect that information about them will be handled respectfully, securely and appropriately.

We are committed to maintaining confidentiality while also recognising that confidentiality is not absolute. Information must be shared when it is necessary to safeguard a child, protect another person, comply with a legal duty or support an authorised safeguarding investigation.

Safeguarding children takes priority over maintaining confidentiality where a child may be at risk of harm.

Information will be:

- obtained and used fairly and lawfully;
- accurate and relevant to its purpose;
- shared only with people who need it;
- limited to the minimum information reasonably necessary;
- recorded appropriately;
- stored securely; and
- retained and disposed of in accordance with the setting's retention arrangements.

2. Purpose

This policy explains:

- how confidential information will be handled;
- when information may or must be shared;
- how safeguarding information will be managed;
- the rules that apply during an open Local Authority Designated Officer investigation;
- the responsibilities of staff, students and volunteers;
- how breaches of confidentiality will be managed; and
- how the setting will balance privacy rights with its safeguarding duties.

3. Scope

This policy applies to:

- employees;
- owners, directors, trustees and committee members;
- agency and supply workers;
- apprentices;
- students on placement;
- volunteers;
- contractors and visiting professionals;
- parents and carers who have access to information through an authorised role; and
- any other person working for or on behalf of the setting.

The policy applies to information communicated verbally, in writing, electronically, through photographs or recordings, and through informal or social communication.

4. Relevant framework

This policy should be read and applied alongside the current versions of:

- the Early Years Foundation Stage statutory framework;
- Working Together to Safeguard Children;
- local safeguarding partnership procedures;
- local authority procedures for managing allegations against adults who work with children;
- the UK General Data Protection Regulation;
- the Data Protection Act 2018;
- the Human Rights Act 1998;
- the Children Act 1989 and Children Act 2004;
- The Stacey Pre-School: Safeguarding and Child Protection Policy;
- The Stacey Pre-School: Allegations Against Staff and Volunteers Policy;
- The Stacey Pre-School: Whistleblowing Policy;
- The Stacey Pre-School: Staff Code of Conduct; and
- The Stacey Pre-School Records Retention and Data Protection Policy.

Where this policy conflicts with specific instructions given by children's social care, the police, the Local Authority Designated Officer or another statutory body, the setting will follow the lawful instructions of that body.

5. Definitions

Confidential information

Confidential information includes information that is private, sensitive or not intended for general circulation, including:

- personal information about a child or family;
- health, medical or developmental information;
- safeguarding records;
- information about family circumstances;
- special educational needs or disabilities;
- financial information;
- employee and volunteer records;
- supervision, disciplinary and capability information;
- complaints;
- allegations or concerns about adults working with children;
- information received from another professional or agency; and
- passwords, security arrangements and access information.

Safeguarding information

Safeguarding information includes any information indicating that:

- a child may have suffered or may be at risk of suffering harm;
- a child may require additional help or protection;
- an adult may present a risk to a child;
- a member of staff or volunteer may have behaved in a way that meets or may meet the allegations criteria;
- there may have been a breach of professional boundaries;
- there is a low-level concern about an adult's conduct; or
- a safeguarding plan, assessment or investigation is in progress.

Need to know

"Need to know" means that a person requires particular information to:

- safeguard a child;
- carry out a defined professional responsibility;
- manage an identified risk;
- participate in an authorised investigation;
- implement agreed staffing or supervision arrangements; or
- comply with a lawful instruction or statutory duty.

A person's seniority, curiosity, friendship with those involved or general involvement in the setting does not automatically give them a need to know.

6. General responsibilities

All people covered by this policy must:

- protect confidential information;
- discuss confidential matters only in an appropriate private environment;
- access only information required for their role;
- follow the setting's safeguarding reporting procedures;
- avoid gossip, speculation and unnecessary discussion;
- use secure systems and approved communication channels;
- report accidental or deliberate information breaches promptly;
- return or securely dispose of records when instructed; and
- continue to respect confidentiality after leaving the setting.

Staff must not promise a child or adult that information will be kept completely secret. They should explain that information may need to be passed to a person who can help keep the child or another person safe.

7. Safeguarding takes priority

Concerns about confidentiality must never prevent a person from reporting a safeguarding concern.

Any member of staff, student or volunteer who:

- is concerned about a child;
- receives a disclosure;
- witnesses concerning conduct;
- becomes aware of new information about an allegation;
- believes an adult may pose a risk to children; or
- believes a concern has not been managed appropriately,

must report the information immediately in accordance with the Safeguarding and Child Protection Policy.

Concerns should normally be reported to the Designated Safeguarding Lead, setting manager or other designated person.

Concerns about the manager must be reported through the route specified in the Allegations Against Staff and Volunteers Policy, which may include direct contact with the Local Authority Designated Officer.

Reporting a concern through the correct safeguarding route is not a breach of confidentiality.

8. Principles for sharing safeguarding information

When deciding whether and how to share information, the setting will consider whether sharing is:

- necessary for the purpose;
- proportionate to the level of risk;
- relevant to the recipient's responsibilities;
- accurate and sufficiently up to date;
- limited to what the recipient needs to know;
- shared securely; and
- appropriately recorded.

Consent may be sought where it is appropriate and safe to do so. However, consent is not always required before sharing information for safeguarding purposes.

Information may be shared without consent where, for example:

- a child may be at risk of harm;
- seeking consent could increase risk;
- seeking consent could prejudice an investigation;
- a person may be placed at risk;
- the information is required by law;
- a statutory agency has lawfully requested it; or
- there is another lawful safeguarding basis for sharing it.

Where there is uncertainty, the Designated Safeguarding Lead or manager should obtain advice from the relevant safeguarding agency, local authority or data-protection adviser. Urgent protective action must not be delayed solely because consent or advice cannot immediately be obtained.

9. Internal sharing of safeguarding concerns

Safeguarding information must not be shared routinely with the whole staff team.

The Designated Safeguarding Lead or manager will decide which members of staff require information to:

- meet a child's immediate needs;
- recognise and respond to identified risks;
- implement a safety or support plan;
- observe and accurately record specified matters;
- maintain required supervision;
- manage staff deployment; or
- fulfil another defined safeguarding responsibility.

Staff receiving limited safeguarding information must:

- use it only for the purpose for which it was shared;
- not seek additional information out of curiosity;
- not discuss it with colleagues unless authorised;
- not approach or question the child, family or person concerned unless instructed;
- record relevant observations factually; and
- report new information through the agreed safeguarding route.

General staff briefings should not identify a child, family or staff member unless identification is genuinely necessary to manage a risk.

10. Confidentiality during an open LADO investigation

10.1 General principle

Where an allegation or concern about an adult working or volunteering with children has been referred to the Local Authority Designated Officer, information about the matter must be treated as strictly confidential.

The fact that an investigation is taking place does not permit staff to discuss the allegation among themselves.

Information will be shared only:

- on a need-to-know basis;
- with the knowledge or authority of the setting's case manager;
- in accordance with advice from the LADO, police or children's social care; and
- for a clear safeguarding, employment or investigative purpose.

The setting's case manager will normally be the Pre-School Manager Where the allegation concerns that person, an alternative case manager will be appointed in accordance with local procedures.

10.2 What staff must do

During an open LADO process, all staff, students and volunteers must:

- continue to report any new safeguarding concern or relevant first-hand information immediately;
- make a factual, signed and dated record where requested;
- preserve any relevant records, messages, documents or other information;
- follow any temporary safeguarding, supervision or deployment arrangements;
- cooperate with authorised enquiries;
- maintain an open mind;
- protect the privacy and dignity of the child and adult concerned; and
- follow instructions given by the case manager or relevant statutory agency.

A staff member who witnessed an incident or holds relevant information may discuss it with the case manager, LADO, police, social worker, authorised investigator or their own authorised representative as appropriate.

10.3 What staff must not do

Unless specifically authorised as part of the investigation, staff must not:

- discuss the allegation or investigation with colleagues;
- compare accounts or statements;
- ask another witness what they saw, heard or reported;
- attempt to agree or reconcile different accounts;
- question or re-interview the child;
- question the person who is the subject of the allegation;
- question parents, carers or other potential witnesses;
- conduct their own investigation;
- search for evidence outside their normal duties;
- speculate about whether the allegation is true or false;
- express opinions about guilt, innocence, motive or likely outcome;
- disclose the identity of the child, family, complainant, witness or adult concerned;
- share information through personal messages, staff messaging groups or social media;

- access safeguarding, personnel or electronic records without authority;
- repeat rumours or unverified information; or
- make comments that could prejudice the investigation or cause distress.

These restrictions apply inside and outside the workplace and continue after the investigation has concluded where the information remains confidential.

10.4 New or additional concerns

Nothing in this section prevents or discourages staff from reporting a new concern.

If a staff member becomes aware of new information, witnesses further concerning behaviour or remembers relevant first-hand information, they must:

- report it promptly to the designated person;
- distinguish clearly between what they personally observed, what they were told and what they have inferred;
- use the person's own words where possible;
- avoid discussing the information with other witnesses; and
- make a factual record as directed.

Staff must not withhold safeguarding information because they believe it is already known, because an investigation is open or because they are concerned about breaching confidentiality.

10.5 Authorised staff communication

The case manager may provide staff with limited information where necessary to:

- maintain the safety and wellbeing of children;
- explain a change in staffing or supervision;
- maintain the safe operation of the setting;
- control rumours or misinformation;
- enable an identified member of staff to provide authorised support; or
- implement instructions agreed with the LADO.

Any communication must be brief, factual and limited to what recipients need to know.

A suitable instruction may be:

> *"A confidential safeguarding process is being managed under the setting's procedures. Temporary arrangements have been put in place. Staff must not speculate or discuss the matter. Any new, relevant information must be reported immediately to [named role]."*

Staff must not interpret limited operational information as permission to seek or share further details.

10.6 Meetings and group discussions

An open allegation must not be discussed during:

- general staff meetings;
- team briefings;
- informal supervision between colleagues;
- breaks or staff-room conversations;
- group messaging;
- training sessions; or
- parent or committee discussions,

unless the case manager has specifically authorised the discussion and established that each participant has a genuine need to know.

Where an authorised meeting is necessary:

- attendance will be restricted;
- the purpose and boundaries of the discussion will be explained;
- only relevant information will be considered;
- speculation will be stopped;
- an appropriate confidential record will be made; and
- attendees will be reminded not to discuss the matter elsewhere.

10.7 Contact with the person subject to the allegation

The person who is the subject of the allegation must be treated fairly and with dignity.

Staff must not:

- confront them about the allegation;
- ask them for an explanation;
- offer or seek details about witness accounts;
- pressure them to resign or withdraw;
- share confidential information with them;
- promise a particular outcome; or
- exclude or isolate them beyond arrangements authorised by management.

Normal professional courtesy may continue unless a risk assessment or instruction states otherwise.

The person may be offered an appropriate named contact or welfare support arrangement. The support person must not be a witness where this could create a conflict and must understand the limits of their role and confidentiality.

10.8 Contact with the child and family

Staff must not initiate discussion with the child or family about the allegation unless authorised.

Where the child raises the matter spontaneously, staff should:

- listen calmly;
- avoid leading or investigative questions;
- not promise secrecy;
- reassure the child that they have done the right thing by speaking;
- make an accurate record;
- report the information immediately; and
- avoid discussing the disclosure with colleagues who do not need to know.

Communication with parents or carers will be managed by the case manager in consultation with the LADO and, where applicable, police or children's social care.

10.9 Information about suspension or absence

Suspension is a neutral act and must not be presented as evidence that an allegation is true.

Where a member of staff is absent, suspended, redeployed or subject to additional supervision, colleagues will be told only what is operationally necessary.

Staff must not speculate about the reason for an individual's absence or communicate assumptions to children, families or other people.

10.10 Parents, carers and external enquiries

Questions from parents, carers, the media or members of the public must be referred to [manager/owner/designated spokesperson].

Staff must not provide comments, confirm identities or state that a LADO referral or investigation exists unless authorised.

Any agreed statement will be factual, proportionate and consistent with advice from the LADO or investigating agencies.

10.11 Social media and electronic communication

- No person covered by this policy may post, send, forward, "like," react to or comment on information relating to an allegation or LADO investigation through:
- social media;
- private messaging;
- personal email;
- online forums;
- community or parent groups; or
- any other unauthorised communication channel.

This includes indirect comments, hints, coded references or information that could allow a person to be identified.

Screenshots, photographs, audio recordings and documents relating to the matter must not be taken, copied or retained on personal devices.

10.12 Conclusion of the process

The case manager will decide, with advice from the LADO where appropriate, what information may be shared once the process concludes.

Staff will not automatically be entitled to know:

- the full evidence considered;
- personal information about those involved;
- confidential employment action;
- medical information;
- the details of police or social-care decisions; or
- the complete rationale for the outcome.

Staff may be given sufficient information to understand any operational changes, safeguarding learning or revised procedures. Any learning discussion must be managed in a way that does not unnecessarily identify or blame individuals. The duty of confidentiality continues after the conclusion of the investigation.

11. Allegations, low-level concerns and whistleblowing

Staff must understand the distinction between:

- an allegation that may meet the LADO criteria;
- a low-level concern about adult conduct;
- a complaint;
- a grievance; and
- a whistleblowing disclosure.

Staff are not expected to decide definitively which procedure applies before reporting a concern. They must pass the information promptly to the person designated by the relevant policy.

Information about low-level concerns must also be kept confidential and shared only with authorised people. Staff must not use the low-level concerns process to investigate, confront or informally discuss another employee's behaviour.

A staff member who believes that a safeguarding concern is being ignored, concealed or managed improperly should use the escalation or whistleblowing procedures. They may contact an appropriate external safeguarding or regulatory body where necessary.

12. Information concerning children and families

Information about children and families will normally be shared with staff only where it is relevant to the care, learning, development, inclusion or safeguarding of the child.

Staff must not:

- discuss children or families in public areas;
- discuss one family with another family;
- disclose addresses, telephone numbers or personal circumstances;
- take records home without authority;
- retain children's information on personal devices;
- share photographs or recordings outside approved systems;
- use information gained through work for a personal purpose; or
- access the record of a child for whom they have no professional responsibility.

Where a parent asks to see information, the request must be passed to the manager or data-protection lead. Staff must not hand over records informally.

Information concerning one person may also contain information concerning another person. The setting will consider the rights and safety of everyone identified before providing access.

13. Conversations and the physical environment

Confidential conversations must take place in an appropriate private location wherever possible.

Staff must take care when:

- speaking at reception or collection times;
- making telephone calls;
- holding meetings where conversations may be overheard;
- displaying information on noticeboards or screens;
- carrying paper records;
- working in shared spaces; and
- discussing children during outings or transport.

Where an urgent safeguarding discussion must take place immediately, staff should move to the most private safe location available and limit the discussion to essential information.

14. Electronic records and communication

Confidential information must be stored and communicated only through systems approved by the setting.

Staff must:

- keep passwords secure;
- lock screens when unattended;
- check recipients before sending information;
- use blind-copy functions appropriately for group emails;
- avoid personal email accounts unless explicitly authorised in an emergency;
- not store records permanently on local devices unless approved;
- report misdirected emails or messages immediately;
- use secure transfer arrangements where required; and
- comply with the setting's mobile-phone, photography and online-safety procedures.

Safeguarding concerns must not be reported solely through a communication method that may not be checked promptly.

15. Record keeping

Records must be:

- clear, factual and legible;
- dated and timed;
- attributed to the person making the record;
- based on observation or information received;
- clear about the source of information;
- written without speculation or inappropriate opinion;
- stored securely; and
- accessible only to authorised people.

Where an error is identified, the original entry must not be obscured or destroyed. Any correction must be identifiable, dated and explained in accordance with the setting's records procedure.

Safeguarding and allegations records will be stored separately from general operational records where appropriate. The setting will record significant information-sharing decisions, including:

- what was shared;
- with whom;
- when and how it was shared;
- the reason for sharing;
- whether consent was obtained or considered;
- any advice received; and
- the outcome or action agreed.

Where a decision is made not to share information despite an identified concern, the reasons must also be recorded.

16. Supervision and staff support

Professional supervision may involve discussion of confidential matters, but it must not be used to circulate gossip or obtain information about a safeguarding investigation.

A supervisor may discuss confidential information only where:

- the discussion is within the scope of their authorised role;
- it supports safe practice or staff welfare;
- it does not compromise an investigation;
- information is limited to what is necessary; and
- any safeguarding information is passed through the correct route.

Where an employee requires emotional support during an investigation, the case manager will identify an appropriate support route. Support arrangements must not allow witnesses to compare evidence or receive confidential details.

Employees may seek independent advice from their trade union, professional association or legal adviser. They remain responsible for sharing information securely and only to the extent necessary to obtain that advice.

17. Students, volunteers and agency staff

Students, volunteers and agency staff are subject to the same confidentiality standards as employed staff.

Before beginning their role, they will be informed:

- what information they may access;
- who they must report concerns to;
- that they must not discuss children or staff outside the setting;
- that safeguarding concerns must always be reported;
- that they must not investigate concerns themselves; and
- that confidentiality continues after their placement or work ends.

Placement tutors, agencies and training providers will receive only information that is relevant and lawful to share.

18. Sharing information with other agencies

The setting will cooperate with lawful safeguarding enquiries and may share relevant information with bodies including:

- children's social care;
- the police;
- the Local Authority Designated Officer;
- Ofsted;
- health professionals;
- the local safeguarding partnership;
- the Disclosure and Barring Service;
- schools and other early years providers; and
- other statutory or professional bodies.

Before routine external sharing, the setting will normally verify:

- the identity and authority of the recipient;
- the purpose of the request;
- the legal or safeguarding basis;
- what information is necessary;
- the appropriate secure method; and
- whether the sharing should be recorded.

Urgent sharing to protect a child must not be delayed by unnecessary administrative requirements.

19. Ofsted notifications

The registered provider will make notifications to Ofsted where required by the EYFS statutory framework and applicable regulations.

Information about an allegation or other significant event will be provided accurately, within the required timescale and through an authorised person.

Staff must not assume that another agency has notified Ofsted unless this has been confirmed.

Ofsted notification does not replace referral to the LADO, police, children's social care or another relevant agency.

20. Disclosure to parents and carers

Parents and carers will normally be given information about their own child, subject to safeguarding, confidentiality and legal considerations.

Information may be withheld temporarily or shared without prior parental knowledge where informing a parent could:

- place a child or another person at risk;
- prejudice a police or safeguarding investigation;
- lead to loss or destruction of evidence;
- cause an avoidable delay in protective action; or
- conflict with instructions from a statutory agency.

The decision and reason will be recorded.

The setting will not disclose confidential information about another child, family or employee when responding to a complaint or request for information.

21. Media enquiries

Only [named role] may speak on behalf of the setting to journalists or media organisations.

All media enquiries relating to children, families, staff allegations or safeguarding matters must be referred immediately to that person.

No staff member may provide information "off the record," anonymously or through a personal account.

22. Breaches of confidentiality

A breach may include:

- unauthorised disclosure;
- gossip or speculation;
- accessing records without a legitimate reason;
- losing confidential information;
- sending information to the wrong recipient;
- discussing an open LADO investigation without authority;
- posting relevant information online;
- failing to secure records;
- withholding safeguarding information; or
- using confidential information for personal advantage.

Any actual or suspected breach must be reported immediately to [manager/data-protection lead/DSL].

The setting will:

- take steps to contain the breach;
- assess risks to affected individuals;
- protect children and others from further harm;
- preserve relevant evidence;
- notify appropriate people or bodies where required;
- record the incident and response; and
- identify any changes needed to practice.

A deliberate or serious breach may result in disciplinary action, termination of placement or contract, referral to a professional body, referral to the Disclosure and Barring Service, regulatory notification or legal action.

A confidentiality rule will not be used to punish a person for making a genuine safeguarding report or protected whistleblowing disclosure through an appropriate route.

23. Training

All staff, students and volunteers will receive information appropriate to their role concerning:

- confidentiality;
- data protection;
- safeguarding information-sharing;
- record keeping;
- allegations against adults;
- the role of the LADO;
- whistleblowing;
- secure electronic communication; and
- responding to information breaches.

Training and induction will emphasise that:

- safeguarding concerns must be reported;
- confidentiality does not mean secrecy;
- staff must not investigate concerns themselves;
- LADO matters must not be discussed informally; and
- only authorised people may decide what information can be shared more widely.

24. Monitoring

The manager will monitor compliance through:

- induction and training records;
- supervision;
- safeguarding record audits;
- access controls;
- data-breach records;
- recruitment and disciplinary records;
- review of information-sharing decisions; and
- feedback from safeguarding agencies where appropriate.

Any pattern of inappropriate sharing, failure to share or insecure record keeping will be addressed promptly.

25. Review

This policy will be reviewed:

- at least annually;
- following a confidentiality or safeguarding incident;
- following a LADO case where organisational learning is identified;
- when legislation or statutory guidance changes;
- when local safeguarding procedures change; or
- when monitoring identifies a need for revision.

The setting will check this policy against its own local authority's LADO procedures because local referral, recording and communication arrangements may differ.