Alpha Inclusion and Communication

Confidentiality policy and procedure

Policy date: September 2025
Review date: November 2026

Rationale:

- The safety, well-being and protection of our children and young people are the paramount considerations in all decisions staff at Alpha Inclusion and Communication make about confidentiality.
- The appropriate sharing of information between company staff is an essential element in ensuring our young people's well-being and safety.
- It is an essential part of the ethos of our company that trust is established to enable young people, staff and parents/carers to seek help both within and outside the company. We therefore, minimise information sharing to those occasions which are appropriate to ensure young people and staff are supported and safe.
- Young people, parents/carers and staff need to know the boundaries of confidentiality in order to feel safe and comfortable in discussing personal issues and concerns.
- The company's attitude to confidentiality is open and easily understood and everyone should be able to trust the boundaries of confidentiality operating within the company.
- Everyone in the company community needs to know that no one can offer absolute confidentiality and that there are limits of confidentiality that can be offered by individuals within the company community – so they can make informed decisions about the most appropriate person to talk to.
- Business interests and information on the company must be protected to ensure it remains at a competitive advantage.

Scope:

This policy affects all employees including board members, investors, contractors and volunteers, who may have access to confidential information.

A. CONFIDENTIALITY WORKING WITH CHILDREN AND YOUNG PEOPLE

Definition of Confidentiality

The dictionary definition of confidential is "Of the nature of confidence; spoken or written in confidence; characterized by the communication of secrets or private matters.'" When speaking confidentially to someone, the confider has the belief that the confidant will not discuss the content of the conversation with another.

The confider is asking for the content of the conversation to be kept secret and not shared with third parties. Anyone offering absolute confidentiality to someone else would be offering to keep the content of his or her conversation completely secret and discuss it with no one.

In practice regarding working with children and young people, there are few situations where absolute confidentiality is offered. We have to strike a balance between ensuring the safety, wellbeing and protection of our young people and staff, ensuring there is an ethos of trust where young people and staff can ask for help when they need it - and ensuring that when it is essential to share confidential information, child protection procedures and good practice are followed. This means that in most cases what is on offer is limited confidentiality.

Disclosure of the content of a conversation could be discussed with professional colleagues but the confider would not be identified except in certain circumstances such as immediate mental or physical safety. The general rule is that staff should make clear at the beginning of the conversation that there are limits to confidentiality. These limits relate to ensuring children's safety and well-being. The young person will be informed when a confidence has to be broken for this reason and will be encouraged to do this for themselves whenever this is possible.

The GDPR and Data Protection Act 2018, **does not** prevent the sharing of information for the purposes of safeguarding children, when it is necessary, proportionate and justified to do so. In fact, data protection legislation provides a framework which enables information sharing in that context. The first and most important consideration is always whether sharing information is likely to support the safeguarding of a child. . To effectively share information:

- all practitioners should be confident of the processing conditions, which allow them to store, and share, the information that they need to carry out their safeguarding role. Information which is relevant to safeguarding will often be data which is considered 'special category personal data' meaning it is sensitive and personal.
- where practitioners need to share special category personal data, they should be aware that the Data Protection Act 2018 includes 'safeguarding of children and individuals at risk' as a condition that allows practitioners to share information without consent
- information can be shared legally without consent, if a practitioner is unable to, cannot be reasonably expected to gain consent from the individual, or if to gain consent could place a child at risk.
- relevant personal information can be shared lawfully if it is to keep a child or individual at risk safe from neglect or physical, emotional or mental harm, or if it is protecting their physical, mental, or emotional well-being.

Three different levels of confidentiality are appropriate for different circumstances.

1. In group work in the course of a session given by a member of staff or an outside visitor, including health professionals. Careful thought needs to be given to the content of the session, setting the climate and establishing ground rules to ensure confidential disclosures are not made. It should be made clear to young people that this is not the time or place to disclose confidential, personal information. When another professional is contributing to a company health programme in a session they are working with the same boundaries of confidentiality as a staff member.
2. One to one disclosures to members of company staff (including voluntary staff). It is essential all members of staff know the limits of the confidentiality they can offer to both young people and parents/carers (see note below and safeguarding policy) and any required actions and sources of further support or help available, both for the young person or parent/carer and for the staff member within the company. This includes support/advice from other agencies, where appropriate. All staff at this company encourage young people to discuss difficult issues with their parents or carers, and vice versa. However, the needs of the young person are paramount and company staff will not automatically share information about the young person with their parents/carers unless it is considered to be in the child's best interests. Note: when concerns for a child or young person come to the attention of staff, for example through observation of behaviour or injuries or disclosure, however insignificant this might appear to be, the member of staff should discuss this with one of the Designated Safeguarding Leads as soon as possible. More serious concerns must be reported immediately to ensure that any intervention necessary to protect the child is accessed as early as possible. Please see the company Safeguarding Policy.
3. Confidential company information (see more information below).

The legal position for company staff:

Company staff (including non-practitioners and voluntary staff) should not promise confidentiality to children and young people. Young people do not have the right to expect that incidents will not be reported to their parents/carers and may not, in the absence of an explicit promise, assume that information conveyed outside that context is private.

No member of this company's staff can or should give such a promise. The safety, well-being and protection of the child is the paramount consideration in all decisions staff at this company make about confidentiality. Company staff are not obliged to break confidentiality except where child protection is or may be an issue, however, at Alpha Inclusion and Communication we believe it is important staff are able to share their concerns about young people with colleagues in a professional and supportive way, on a need-to-know basis, to ensure staff receive the guidance and support they need and the young people' safety and well-being is maintained.

Company staff should discuss such concerns with the DSP (Designated Safeguarding Person) in the school in the first instance or the company DSP if the concern is outside of a school environment.

Where there are concerns about the safety of a child, the sharing of information in a timely and effective manner between organisations can improve decision-making so that actions taken are in the best interests of the child. The GDPR and Data Protection Act 2018 place duties on organisations and individuals to process personal information fairly and lawfully; they are not a barrier to sharing information, where the failure to do so would cause the safety or well-being of a child to be compromised. Similarly, human rights concerns, such as respecting the right to a private and family life would not prevent sharing where there are real safeguarding concerns.

Guardians and Outreach Staff:

Professional judgement is required by a Guardian and Systematic Practitioner in considering whether he or she should indicate to a child that the child could make a disclosure in confidence and whether such a confidence could then be maintained having heard the information. In exercising their professional judgement the staff member must consider the best interests of the child including the need to both ensure trust to provide safeguards for our children and possible child protection issues.

All staff at Alpha Inclusion and Communication receive basic training in child protection as part of their induction to this company and are expected to follow the Safeguarding Policy and procedures. Any concerns should be discussed with the Designated Safeguarding Person within the host school or, in the case of family and community work, with the company DSP.

Fears about sharing information cannot be allowed to stand in the way of the need to safeguard and promote the welfare of children at risk of abuse or neglect. Every practitioner must take responsibility for sharing the information they hold, and cannot assume that someone else will pass on information, which may be critical to keeping a child safe.

Visitors, Volunteers and non-practitioners:

At Alpha Inclusion and Communication we expect all staff, including voluntary staff, to report any disclosures by young people or parents/carers, of a concerning personal nature to the Designated Safeguarding Person at the host school or the company DSP as soon as possible after the disclosure and in an appropriate setting, so others cannot overhear. This is to ensure the safety, protection and well-being of all our young people and staff. The Designated Safeguarding Lead will decide what, if any, further action needs to be taken, both to ensure the young person gets the help and support they need and that the member of staff also gets the support and supervision they need.

Parents/carers:

Alpha Inclusion and Communication believes that it is essential to work in partnership with parents and carers and we endeavour to keep parents/carers abreast of their child's progress at the company, including any concerns about their progress or behaviour. However, we also need to maintain a balance so that our young people can share any concerns and ask for help when they need it. Where a pupil does discuss a difficult personal matter staff at company, they will

be encouraged to also discuss the matter with their parent or carer themselves (if appropriate and safe to do so).

The safety, well-being and protection of our young people is the paramount consideration in all decisions staff at this company make about confidentiality.

Complex cases:

Where there are areas of doubt about the sharing of information, a consultation should be sought with the local Children's Safeguards Service Child Protection Co-ordinator (information through the Designated Safeguarding Lead).

Ground Rules to be used in sessions:

The Behaviour Charter for Children and Young People sets out the expectations to ensure a safe environment for learning.

This reduces anxiety to young people and staff and minimises unconsidered, unintended personal disclosures. Alongside this practitioners should remind young people not to share things they want to keep confidential and that they can pass or opt out of something if it makes them feel uncomfortable.
If we do find out things about other young people, which are personal and private, we won't talk about it outside the session, but if we are worried about someone else's safety we tell a teacher or other school staff member.

When confidentiality should be broken and procedures for doing this:

- See the Safeguarding Policy – generally any situation where the health, well-being or safety of a child are in question.
- Where this does not apply and you are still concerned and unsure of whether the information should be passed on or other action taken you should speak to either the Team Lead or Manager.
- If the Team Lead issues instructions that they should be kept informed, all staff must comply. There is always a good reason for this, which you may not know about.

The seven golden rules to sharing information

1. Remember that the General Data Protection Regulation (GDPR), Data Protection Act 2018 and human rights law are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately.
2. Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
3. Seek advice from other practitioners, or your information governance lead, if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.

4. Where possible, share information with consent, and where possible, respect the wishes of those who do not consent to having their information shared. Under the GDPR and Data Protection Act 2018 you may share information without consent if, in your judgement, there is a lawful basis to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be clear of the basis upon which you are doing so. Where you do not have consent, be mindful that an individual might not expect information to be shared.
5. Consider safety and well-being: base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.
6. Necessary, proportionate, relevant, adequate, accurate, timely and secure: ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (see principles).
7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Principles of Confidential Discussion:

- Ensure the time and place for a discussion are appropriate. When they are not, we reassure the young person that we understand that they need to discuss something very important and that it warrants time, space and privacy. See the young person normally (and always in cases of neglect, or abuse) before the end of the day. More serious concerns must be reported immediately to the school's Senior Designated Safeguard Lead to ensure that any intervention necessary to protect the child/ young person is accessed as early as possible.
- Tell the child we cannot guarantee confidentiality if we think they will:
    - hurt themselves
    - hurt someone else
    - or they tell us that someone is hurting them or others
- Do not interrogate the child or ask leading questions.
- Do not put children in the position of having to repeat distressing matters to several people but we will inform the pupil first before any confidential information is shared, with the reasons for this.
- Encourage the young person, whenever possible, to confide in their own parents/carers

Support for staff:

Staff may have support needs themselves in dealing with some of the personal issues of our young people. At Alpha Inclusion and Communication we prefer you to ask for help rather than possibly making a poor decision because you don't have all the facts or the necessary training or taking worries about young people home with you.

There are many agencies schools can refer young people to who need additional support and they have procedures to ensure this happens. We work alongside schools and other agencies as part of a team to support our young people and asking for help is a way. We also ensure all staff have supervision sessions to support them.

All Alpha Inclusion employees receive training in NVC (non-violent communication) and undertake regular dee-brief training to allow them to access support from colleagues whilst maintaining confidentiality.

Onward referral

The Inclusion Manager or Senior Designated Safeguarding Lead in the school is normally responsible for referring young people to outside agencies.

If there is an emergency safeguarding concern, following a discussion, and school and company DSLs are unavailable, advice should be sort from the Area Safeguarding Officer and/or the Central Duty Team).

B. CONFIDENTIALITY REGARDING PERSONAL INFORMATION OF STAFF AND COLLEAGUES

All staff have the right to privacy regarding their personal information, including but not limited to their health, family circumstances, contact details, employment status, and any matters relating to performance or conduct. Such information must only be accessed, discussed, or shared where there is a legitimate professional need to do so and only with those authorised to receive it. Staff must not disclose or discuss another colleague's personal information in any informal or public setting, including but not limited to, shared work spaces, on social media or with individuals outside the organisation. Further information on how information is stored and shared is detailed in the GDPR and Data Protection Policy Breaches and the Employee Privacy Notice. Breaches of confidentiality relating to staff personal information will be treated seriously and may result in disciplinary action.

C. CONFIDENTIALITY REGARDING COMPANY INFORMATION

Knowledge Assets and Intellectual Property Knowledge Assets (KAs) are intangible assets that have an inherent value to an organisation. KAs include intellectual property that an organisation holds, the skills and experience of its staff and its reputation. These include inventions, designs, certain R&D outcomes, data and information, creative outputs such as text, video, graphics, codified knowledge such as software and source code, know-how and expertise, business processes, services and other intellectual resources. It may also include anything that is protected by UK or international intellectual property rights (patents, trademarks, registered or unregistered designs and copyright), trade secrets, which have their own form of legal protection, and contractual and non-contractual relationships.

What is Intellectual Property? Intellectual property or IP is all around you. It cannot be seen or touched but as a civil or public servant it's likely you will create, handle, or manage IP every day. IP is the collective term used to describe creations of the mind. For example: a story, an invention, an artistic work or a symbol. IP is something that you will create, handle, or manage every day. The main types are patents, trade marks, designs and copyright.

Confidential and proprietary information is secret, valuable, expensive and/or easily replicated.

Common examples of confidential information are:

- Internal company procedures and interventions
- Unpublished financial information
- Data of Clients/Partners/Vendors/ Staff
- Patents or new technologies
- Customer lists (existing and prospective)
- Data entrusted to our company by external parties
- Pricing/marketing and other undisclosed strategies
- Documents and processes explicitly marked as confidential
- Unpublished goals, forecasts and initiatives

Employees may have various levels of authorized access to confidential information.

What employees should do:

- Lock or secure confidential information at all times
- Shred confidential documents when they're no longer needed
- Make sure they only view confidential information on secure devices
- Only disclose information to other employees when it's necessary and authorized
- Keep confidential documents inside our company's premises unless it's absolutely necessary to move them

What employees shouldn't do:

- Use confidential information for any personal benefit or profit
- Disclose confidential information to anyone outside of our company
- Replicate confidential documents and files and store them on insecure devices

When employees stop working for our company, they're obliged to return any confidential files and delete them from their personal devices.

Confidentiality Measures

We'll take measures to ensure that confidential information is well protected. We'll:

- Store and lock paper documents
- Encrypt electronic information and safeguard databases
- Ask employees to sign non-compete and/or non-disclosure agreements (NDAs)
- Ask for authorization by senior management to allow employees to access certain confidential information
- Follow General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) at all times

Exceptions

Confidential information may occasionally have to be disclosed for legitimate reasons. Examples are:

- If a regulatory body requests it as part of an investigation or audit
- If our company examines a venture or partnership that requires disclosing some information (within legal boundaries)

In such cases, employees involved should document their disclosure procedure and collect all needed authorizations. We're bound to avoid disclosing more information than needed.

Disciplinary Consequences

Employees who don't respect our confidentiality policy will face disciplinary and, possibly, legal action.

We'll investigate every breach of this policy. We'll terminate any employee who wilfully or regularly breaches our confidentiality guidelines for personal profit. We may also have to follow the disciplinary procedure for any unintentional breach of this policy depending on its frequency and seriousness. We'll terminate any employees who repeatedly disregard this policy, even when they do so unintentionally. This policy is binding even after separation of employment.

Other related company policies and procedures:

This policy is intended to be used in conjunction with our:
Safeguarding, Whistle-Blowing & GDPR & Data Protection policies,
Employee and Client Privacy Notices
Links to external guidance:
This policy should be read in conjunction with the Department for Education's Information Sharing - Advice for practitioners providing safeguarding services for children, young people, parents and carers May 2024
https://assets.publishing.service.gov.uk/media/66320b06c084007696fca731/Info_sharing_advice_content_May_2024.pdf

Dissemination and implementation:

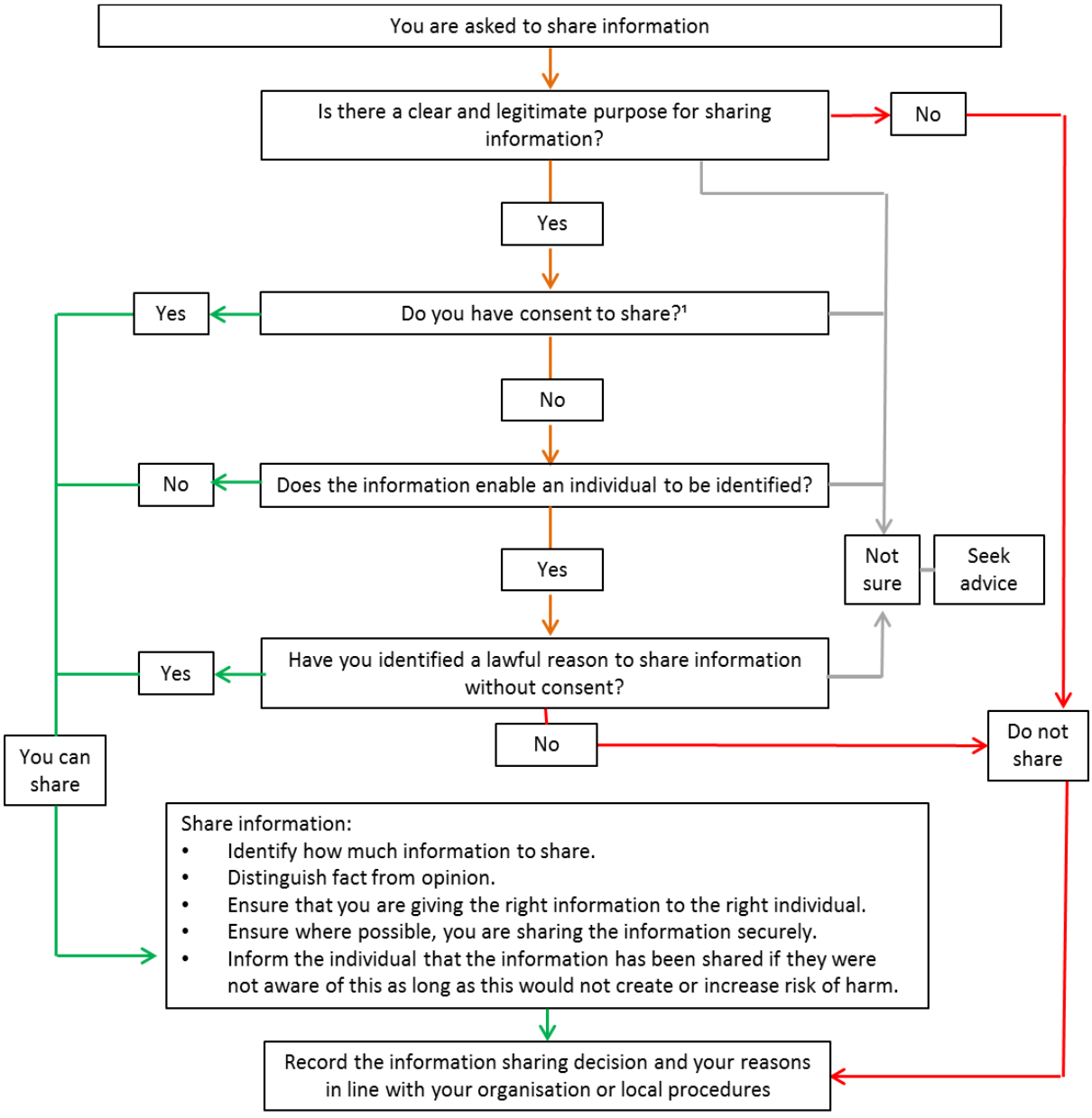
This policy has been distributed to all staff and is discussed in briefings on an annual basis. The policy forms part of the induction process of new staff.

Review

The Management will review this policy and amend it following any major changes in procedure or annually whichever occurs first. Alpha Inclusion & Communication will monitor this policy to ensure that it meets statutory and legal requirements including the GDPR, Data Protection Act, Children's Act, Rehabilitation of Offenders Act, Prevention of Terrorism Act and the Human Rights Act.

Information sharing flowchart

Seek advice from your manager or senior designated person for safeguarding if you are not sure what to do at any stage and ensure that the outcome of the discussion is recorded.



If there are concerns that a child is in need, suffering or likely to suffer harm, then follow the relevant procedures without delay. Seek advice if unsure what to do at any stage and ensure that the outcome of the discussion is recorded.

1. Consent must be unambiguous, freely given and may be withdrawn at any time