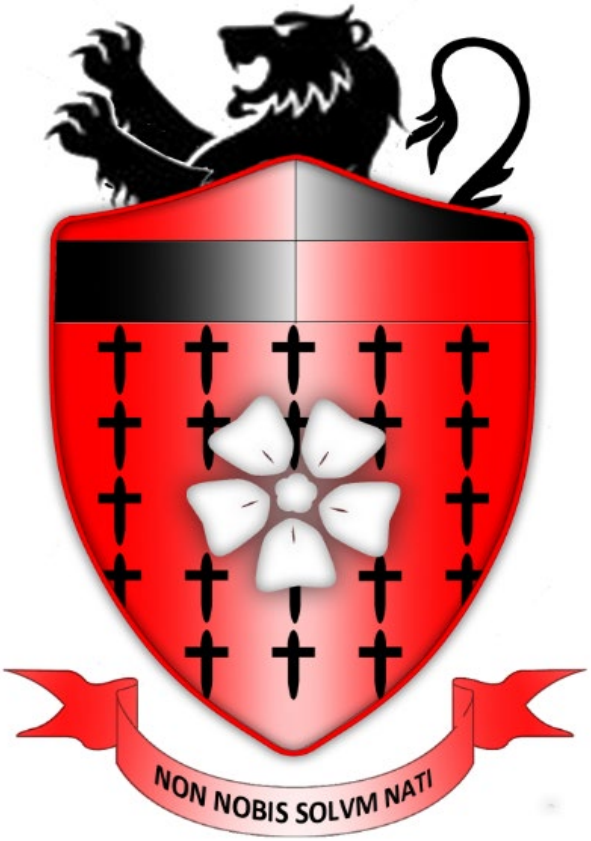
Hornsea School & Language College



Information Sharing Policy

Last Reviewed:	**Date:** September 2024	**By:** Kay Sullivan/Kelly Douse
Approved by:	**Headteacher:** 27.11.24	**Governing Body:** 27.11.24
Date of Next Review:	November 2025	

Information Sharing Policy

This policy links to other HSLC documents:

- Privacy Notice for Parents and Carers
- Retention Schedule
- Personal Data Breach Policy
- Data Protection Policy

Introduction

Information sharing is essential for effective safeguarding and promoting the welfare of children and young people. It is a key factor identified in many serious case reviews (SCRs), where poor information sharing has resulted in missed opportunities to take action that keeps children and young people safe (HM Government: Information sharing Advice for practitioners providing safeguarding services to children, young people, parents and carers July 2018, updated July 2023)

Sharing information is an intrinsic part of any frontline practitioners' job when working with children and young people. The decisions about how much information to share, with whom and when, can have a profound impact on individuals' lives. Information sharing helps to ensure that an individual receives the right services at the right time and prevents a need from becoming more acute and difficult to meet.

Poor or non-existent information sharing is a factor repeatedly identified as an issue in Serious Case Reviews (SCRs) carried out following the death of or serious injury to, a child. In some situations, sharing information can be the difference between life and death.

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.

Professor Munro's review of child protection concluded the need to move towards a child protection system with less central prescription and interference, where we place greater trust in, and responsibility on, skilled practitioners at the frontline.

1. Those skilled practitioners are in the best position to use their professional judgement about when to share information with colleagues working within the same organisation, as well as with those working within other organisations, in order to provide effective early help, to promote their welfare, and to keep children safe from harm. Lord Laming emphasised that the safety and welfare of children is of paramount importance and highlighted the importance of practitioners feeling confident about when and how information can be legally shared.

2. He recommended that all staff in every service, from frontline practitioners to managers in statutory services and the voluntary sector should understand the circumstances in which they may lawfully share information, and that it is in the public interest to prioritise the safety and welfare of children.

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.

At Hornsea School and Language College, we fully accept our responsibility to share information in an appropriate and timely fashion as part of our commitment to safeguarding and ensuring the well-

being of pupils. Information sharing, with parents, partner agencies, pupils and staff is a not only a priority, but a key means of ensuring integrated working across services, intervening early to provide support and preventing any problems escalating. As such, it is rooted in the 'inclusive' approach to education and pupil well-being that characterises the school community.

In the first instance, and wherever appropriate, school will always seek to consult and obtain appropriate consents for sharing any information or making referrals to partner agencies. However, the school recognises that in some circumstances, consent is not the most appropriate lawful basis for sharing or processing information. In these circumstances, the school will ensure that before sharing this information the lawful basis has been determined. Great care is taken within school to ensure that any information shared amongst staff is appropriate and proportionate and on a 'need to know' basis, sufficient to facilitate necessary support.

Please also refer to the school HSLC Strategic Safeguarding and Child Protection Policy and Procedures for additional information on the approach to consent and information sharing in the event of safeguarding concerns. Decisions made in relation to any sharing of information will be fully documented as will the reasons for any such decision making and advice received (e.g. Police and Children's Social care)

Aim

The aim of this policy is to support good practice in information sharing by clarifying how and when information can and should be shared in line with legal and professional obligations. This policy is informed by and based upon the following key documents -

- Working Together to Safeguard Children (December 2023)
- Information Sharing Advice for practitioners providing safeguarding services to children, young people, parents and carers (July 2018)
- Keeping Children Safe in Education (September ~~2023~~2024)
- Children Act 2004
- Young People's Act 2008
- The General Data Protection Regulations and Data Protection Act 2018
- East Riding Safeguarding Children Partnership Procedures and Guidance

This policy is in place to ensure that all members of staff working on the school site are clear about sharing of information and the levels of confidentiality that they can offer to the school community and expect themselves.

The policy was developed following recommendations contained in the documents noted above that encourage the development of a clear policy framework and guidance for practice. The policy is also good practice because:

- A clear, explicit and well publicised Information Sharing policy ensures good practice throughout the school which staff, (including professionals from external agencies), parents/carers and pupils can easily understand. The school needs to be clear about the boundaries of respective legal and professional roles and responsibilities e.g. Child Protection/ safeguarding procedures. Different professionals can offer varying levels of confidentiality in different circumstances and depending upon agency setting (e.g. Health). Sometimes parents/carers and families may wish to disclose information confidentially to the school. The school needs to be clear about its position with regard to limitations and obligations.

Who does the policy apply to?

- All teaching and non-teaching staff employed by the school (including volunteers)
- All visiting staff working with young people on the school site during the school day.
- Depending on their contractual arrangements, staff from external agencies delivering services on the school site
- All members of the Governing Body

All school staff members: Confidentiality and pupils
NB This applies to both teaching and non teaching members of staff, visiting staff and outside agencies

- We recognise that there are occasions when pupils are worried about something and feel that they cannot talk about it to their parents/carers. This can result in enormous stress for the individual which may impact on their education and health. Some pupils may feel that they can turn to teachers and other staff members for support and we want to be as helpful as we can whilst recognising that there may be some potential difficulties in being supportive.
- When talking with pupils, it is important to be aware of maintaining professional boundaries. Whilst being supportive, distancing techniques should be used when appropriate and pupils encouraged or supported to access the targeted support services offered on the school site by school based professionals or agency partners
- **Unconditional confidentiality cannot be offered when a pupil first begins to talk about something where confidentiality may become an issue.**
- Pupils should be warned that if there is a child protection/safeguarding issue where the pupil, or others, are likely to be at risk of significant harm, staff **are under a duty to inform the School's Designated Safeguarding Lead (Kay Sullivan) or the Deputy Designated Safeguarding Lead (Emma Webster) who may have to involve other agencies.** Please refer to the school's Safeguarding and Child Protection Policy and procedures/ for further advice on this aspect). It is important that each member of staff deals with this sensitively and explains to the pupil that they must inform the appropriate people who can help the child, but that they will only tell those who need to know in order to help.
- In all cases where it is felt that confidentiality with the pupil has to be broken, the pupil must be informed, (unless there is a good reason not to inform them e.g. risk of harm) and reassured that their best interests will be maintained.
- In talking with pupils, staff should explore whether or not the student can discuss their difficulty with their parents/carers support in doing this should be offered where appropriate.
- Pupils should be made aware of the specialist targeted services that are available on the school site or in the school community e.g. School Nurse, Early Help and GP.

Role of the Governing Body:

As per KCSiE ~~2023~~ 2024, Governing Bodies and proprietors should ensure relevant staff have due regard to the relevant data protection principles, which allow them to share (and withhold) personal information, as provided for in the Data Protection Act 2018 and the UK GDPR

This includes:

- Being confident of the processing conditions which allow them to store and share information for safeguarding purposes, including information, which is sensitive and personal, and should be treated as 'special category personal data'
- Understanding that 'safeguarding of children and individuals at risk' is a processing condition that allows practitioners to share special category personal data. This includes allowing practitioners to share information without consent where there is a good reason to do so, and that the sharing of information will enhance the safeguarding of a child in a timely manner. It

would be legitimate to share information without consent where; it is not possible to gain consent; it cannot be reasonably expected that a practitioner gains consent; and, if to gain consent would place a child at risk, and

- For schools, not providing pupils' personal data where the serious harm test under the legislation is met. For example, in a situation where a child is in a refuge or another form of emergency accommodation, and the serious harm test is met, they must withhold providing the data in compliance with the school's obligations under the Data Protection Act 2018 and the UK GDPR. Where is doubt, schools should seek independent legal advice.

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.

The General Data Protection Regulation (GDPR) and Data Protection Act 2018

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 introduce new elements to the data protection regime, superseding the Data Protection Act 1998. Practitioners must have due regard to the relevant data protection principles which allow them to share personal information.

The GDPR and Data Protection Act 2018 place greater significance on organisations being transparent and accountable in relation to their use of data. All organisations handling personal data need to have comprehensive and proportionate arrangements for collecting, storing, and sharing information.

The GDPR and Data Protection Act 2018 do not prevent, or limit, the sharing of information for the purposes of keeping children and young people safe.

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

Information Requests

Organisations and agencies within a strong multi-agency system should have confidence that information is shared effectively, amongst and between them, to improve outcomes for children and families. Safeguarding partners may require any person or organisation or agency to provide them, and relevant agency for the area, a reviewer or another person or organisation or agency, with specified information. This must be information which enables and assists the safeguarding partners to perform their functions to safeguard and promote the welfare of children in their area, including as related to local and national child safeguarding practice reviews. The person or organisation to whom a request is made must comply with such a request and if they do not do so, the safeguarding partners may take legal action against them. As public authorities, safeguarding partners should be aware of their own responsibilities under the relevant information law and have regard to guidance provided by the Information Commissioner's Office when issuing and responding to requests for information. (Working Together to Safeguard Children)

Legislative framework

Key organisations who have a duty under section 11 of the Children Act 2004 to have arrangements in place to safeguard and promote the welfare of children are:

- the local authority;
- NHS England;
- clinical commissioning groups;
- NHS Trusts, NHS Foundation Trusts;
- the local policing body;
- British Transport Police Authority;
- prisons;
- National Probation Service and Community Rehabilitation Companies;
- youth offending teams; and
- bodies within the education and /or voluntary sectors, and any individual to the extent that they are providing services in pursuance of section 74 of the Education and Skills Act 2008

There are also a number of other similar duties, which apply to other organisations. For example, section 175 of the Education Act 2002 which applies to local authority education functions and to governing bodies of maintained schools and further education institutions, and section 55 of the

Borders, Citizenship and Immigration Act 2009 which applies to the immigration, asylum, nationality and customs functions of the Secretary of State (in practice discharged by UK Visas and Immigration, Immigration Enforcement and the Border Force, which are part of the Home Office).

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.

All organisations should have arrangements in place, which set out clearly the processes and the principles for sharing information internally. In addition, these arrangements should cover sharing information with other organisations and practitioners, including third party providers to which local authorities have chosen to delegate children's social care functions, and any Local Safeguarding Children Partnerships (LSCP) still operating within the local authority area as well as safeguarding partners (please see below). One approach to aid effective information sharing is the use of Multi-Agency Safeguarding Hubs, where teams may be co-located physically or locally. In these settings, it is important that accountability is defined to ensure that teams know who is responsible for making decisions and that actions taken are in the best interest of the child.

Safeguarding partners (as defined in Section 16E of the Children Act 2004) and LSCPs (where still in operation) should play a strong role in supporting information sharing between and within organisations and addressing any barriers to information sharing. This should include ensuring that a culture of appropriate information sharing is developed and supported as necessary by multi-agency training.

Safeguarding partners and LSCPs (where still in operation) can require a person or body to comply with a request for information, as outlined in sections 16H and 14B of the Children Act 2004, respectively. This can only take place when the information requested is for the purpose of enabling or assisting the safeguarding partners or LSCP to perform their functions. Any request for information to a person or body, should be necessary and proportionate to the reason for the request. Safeguarding partners and LSCps should be mindful of the burden of requests and should explain why the information is needed.

The principles

The principles set out below are intended to help practitioners working with children, young people, parents and carers share information between organisations. Practitioners should use their judgement when making decisions about what information to share, and should follow organisation procedures or consult with their manager if in doubt. The most important consideration is whether sharing information is likely to support the safeguarding and protection of a child.

<u>Necessary and proportionate</u>

When taking decisions about what information to share, you should consider how much information you need to release. Not sharing more data than is necessary to be of use is a key element of the GDPR and Data Protection Act 2018, and you should consider the impact of disclosing information on the information subject and any third parties. Information must be proportionate to the need and level of risk.

<u>Relevant</u>

Only information that is relevant to the purposes should be shared with those who need it. This allows others to do their job effectively and make informed decisions. Adequate Information should be

adequate for its purpose. Information should be of the right quality to ensure that it can be understood and relied upon.

Accurate

Information should be accurate and up to date and should clearly distinguish between fact and opinion. If the information is historical then this should be explained.

Timely

Information should be shared in a timely fashion to reduce the risk of missed opportunities to offer support and protection to a child. Timeliness is key in emergency situations and it may not be appropriate to seek consent for information sharing if it could cause delays and therefore place a child or young person at increased risk of harm. Practitioners should ensure that sufficient information is shared, as well as consider the urgency with which to share it.

Secure

Wherever possible, information should be shared in an appropriate, secure way. Practitioners must always follow their organisation's policy on security for handling personal information.

Record

Information sharing decisions should be recorded, whether or not the decision is taken to share. If the decision is to share, reasons should be cited including what information has been shared and with whom, in line with organisational procedures. If the decision is not to share, it is good practice to record the reasons for this decision and discuss them with the requester. In line with each organisation's own retention policy, the information should not be kept any longer than is necessary. In some rare circumstances, this may be indefinitely, but if this is the case, there should be a review process scheduled at regular intervals to ensure data is not retained where it is unnecessary to do so.

When and how to share information

When asked to share information, you should consider the following questions to help you decide if, and when, to share. If the decision is taken to share, you should consider how best to effectively share the information. A flowchart follows the text.

When

Is there a clear and legitimate purpose for sharing information?
• Yes – see next question
• No – do not share

Do you have consent to share?
• Yes – you can share but should consider how
• No – see next question

Does the information enable an individual to be identified?
• Yes – see next question
• No – you can share but should consider how

Have you identified a lawful reason to share information without consent?
• Yes – you can share but should consider how
• No – do not share

How

• Identify how much information to share
• Distinguish fact from opinion
• Ensure that you are giving the right information to the right individual
• Ensure where possible that you are sharing the information securely
• Where possible, be transparent with the individual, informing them that that the information has been shared, as long as doing so does not create or increase the risk of harm to the individual.

All information sharing decisions and reasons must be recorded in line with your organisation or local procedures. If at any stage you are unsure about how or when to 12 share information, you should seek advice on this. You should also ensure that the outcome of the discussion is recorded.

The school nurse and school based health service: Confidentiality and pupils

The government has recognised that for some young people, unless they are able to speak to someone confidentially away from their family, their health and well-being can be at great risk.

Health services (including doctors, our school nurse and health drop-in) can offer confidential health services (including contraception) to pupils under the age of 16 providing they follow the established guidance and protocols in relation to Fraser Guidelines which require:

- The young person understands the advice and has sufficient maturity to appreciate what is involved in terms of moral, legal, social and emotional implications for themselves.
- They cannot be persuaded to tell their parents/carers, or allow them to be informed.
- (If appropriate) they are likely to begin or continue having sex.
- The young person's physical or mental health is likely to suffer unless they receive advice or treatment.
- It is in the young person's best interests to give advice or treatment.

The requirement to offer a confidential service is within the professional Code of Practice for school nurses and other health service staff. The government has also signed up to international legislation and charters which entitle young people to access health services. However, health professionals like everyone else, must inform appropriate services if they become aware of a child protection/ safeguarding issue in discussions with a young person.

NB Onsite services are requested to be very clear in their publicity about the levels of confidentiality offered e.g. Early Help Practitioners or school based health service will be able to offer more confidentiality than will be offered by school staff.

Privacy Notice (How we use Child in Need and Looked After Child information)

The categories of this information that we collect, process, hold and share include:

- personal information (such as name, date of birth and address)
- characteristics (such as gender, ethnicity and disability)
- information relating to episodes of being a child in need (such as referral information, assessment information, Section 47 information, Initial Child Protection information and Child Protection Plan information)
- episodes of being looked after (such as important dates, information on placements)
- outcomes for looked after children (such as whether health and dental assessments are up to date, strengths and difficulties questionnaire scores and offending)
- adoptions (such as dates of key court orders and decisions)
- care leavers (such as their activity and what type of accommodation they have)

Why we collect and use this information

We use this personal data to:

- support these children and monitor their progress
- provide them with pastoral care
- assess the quality of our services
- evaluate and improve our policies on children's social care

The lawful basis on which we use this information

We collect and process information about children in our care and children to whom we provide services under [insert the lawful basis for processing children looked after information for general purposes (must include a basis from Article 6, and one from Article 9 where data processed is special category data from the GDPR-from 25 May 2018)]

Collecting this information

Whilst the majority of children looked after information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the data protection legislation, we will inform you whether you are required to provide certain information to us or if you have a choice in this.

Storing this information

All data held for children in need and children looked after is from date of birth + 25 years in line with our retention policy.

Who we share this information with?

We routinely share this information with:

- the Department for Education (DfE)

Why we share this information

Department for Education (DfE) - We share children in need and children looked after data with the Department on a statutory basis, under Section 83 of 1989 Children's Act, Section 7 of the Young People's Act 2008 and also under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.
This data sharing helps to develop national policies, manage local authority performance, administer and allocate funding and identify and encourage good practice.

We do not share information about our children in need or children looked after with anyone without consent unless the law and our policies allow us to do so.

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education go to:

Children looked after: https://www.gov.uk/guidance/children-looked-after-return

Children in need: https://www.gov.uk/guidance/children-in-need-census

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about children in England. It provides invaluable information on the background and circumstances on a child's journey and evidence on educational performance to inform independent research, as well

as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our children to the DfE as part of statutory data collections. Some of this information is then stored in the national pupil database (NPD). The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, parents, carers and children have the right to request access to information about them that we hold. To make a request for your personal information [please contact our Data Protection Officer at office@hslc.co.uk].

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/