UK Government

Multi-Agency Information Sharing: Tier 1 Data Sharing Agreement (DSA)

For safeguarding organisations and their practitioners

Contents

Table of figures

Summary

This publication provides a non-statutory framework from the Department for Education. It has been produced to help safeguarding organisations and their practitioners to write a Data Sharing Agreement in order to share information for the purposes of safeguarding and promoting the welfare of children.

Who this publication is for

The duty to share information applies to the bodies listed in Section 11(1) of the Children Act 2004 and designated childcare and education agencies under Section 16E. Note designated childcare and education agencies will not be in scope until s2 of the Children's Wellbeing and Schools Act, which amends s16E of the Children Act 2004, is commenced. Where these bodies commission others to deliver safeguarding or welfare services—such as primary care providers—the duty will also apply to those service providers. UK government departments and independent non-departmental government bodies responsible for protecting children and/or regulating data protection therefore set out policy, legislation, and statutory guidance on how the protection system should work and considerations for data protection compliance. Those pieces of legislation assist the relevant sharing partners to evidence their compliance with data protection obligations when sharing information.

Main points

This template is illustrative, for general information only, and does not constitute legal advice. Organisations should adapt this template to their circumstances and remain responsible for their own legal compliance. This template does not replace guidance from the Information Commissioner's Office (and future Information Commission) including the ICO's 10 step guide to sharing information to safeguard children and Data sharing: a code of practice and is modelled on it. While this template provides a framework to support lawful and secure information sharing between safeguarding partners, where one or more organisations have not yet become signatories, or its provisions may need review, this should not be seen as an obstacle to sharing information.

Information sharing is not dependent on a child meeting a specific statutory threshold for services, including significant harm, and should support early identification, prevention, and timely intervention. In emergency or urgent cases, it may not be possible to follow usual processes. In such circumstances, a proportionate approach should be taken, with decision making documented. Practitioners should keep a clear record of what information was shared, with whom and why, and record decisions and the rationale where information is not shared. This should be done as soon as possible.

Section 16E (1) Children Act 2004 places a duty on specified safeguarding partners to make arrangements for the purpose of safeguarding and promoting the welfare of

children in the area. Working Together to Safeguard Children, 2026 sets the expectation that arrangements ensure that, at a local level, organisations and agencies are clear about how they will work together to safeguard all children and promote their welfare. Including:

- How information is shared, sought, analysed, and broken down by protected characteristics to facilitate more accurate and timely decision-making for children and families, and through this the identification of groups of children who may be disproportionately over- or under-represented in services, to understand outcomes for different communities of children

- How effective collection, sharing and analysis of data enables early identification of new safeguarding risks, issues, emerging threats, and joined-up responses across relevant agencies, including the identification of groups of children who may be disproportionately over- or under-represented in services, so that services are adapted to address these issues.

To achieve that safeguarding partners need to share information to ensure they have an up-to-date understanding of what life is like for each child within their area that is as full as possible. Each of them will have various parts of the picture and different frequency of contact to contribute towards that. A fear of sharing special category data must not be a blocker to safeguarding and promoting the welfare of children.

Further to the requirement above, measures in the Children's Wellbeing and Schools Act introduce a clear legal duty to share information for the purposes of safeguarding and promoting the welfare of children, and provision for a Single Unique Identifier or as it is termed in the Act a Consistent Identifier, to be specified and the organisations required to use it via regulations.

Introduction

This template has been established to assist parties to agree at a strategic level effective arrangements for multiagency information sharing for the purposes of safeguarding and promoting the welfare of children. It sets out a template to help parties to consider and set out their shared principles, responsibilities, and expectations of one another, to provide a clear framework to support routine, regular and ad hoc information sharing, consistent decision making, and accountability. In doing so, it seeks to reduce barriers to timely information sharing, strengthen practitioner confidence, support earlier intervention, and enable partners to build a fuller picture of risk, need and outcomes for children and families across the local area.

For the purposes of this template, the terms data and information are closely related and may be used interchangeably in line with safeguarding practice and ICO guidance. Where the Tier 1 Data Sharing Agreement refers to information, this should be understood to include data that may be raw, structured, analysed, or interpreted, and which may or may not constitute personal data. Where the Tier 1 Data Sharing Agreement refers specifically to personal data, special category data, or criminal offence data, those terms have the meanings set out in UK data protection legislation and the relevant provisions of this Tier 1 Data Sharing Agreement apply accordingly.

The partners of this Tier 1 Data Sharing Agreement are aware and understand their legal responsibilities to deliver safeguarding to the entire population as defined (amongst others) in the:

Children Act 1989 (as amended)

A key principle of the 1989 Act is that children are best looked after within their families, with their parents playing a full part in their lives, unless compulsory intervention in family life is necessary. That principle is reflected in:

(a) the concept of parental responsibility.

(b) the ability of unmarried fathers to share that responsibility by agreement with the mother, by joint registration at birth or by court order.

(c) the local authority's functions to provide services which support children and their families.

(d) the local authority's duty to return a looked after child to his/her family unless this is against his/her interests; and

(e) the local authority's duty, unless it is not reasonably practicable or consistent with his/her welfare, to endeavour to promote contact between a looked after child and his/her parents or others.

Children Act 2004, Section 10

Each local authority must make arrangements to promote co-operation between partners (including the ICB, Police, Schools and other) to improve the wellbeing of children including:

(a)physical and mental health and emotional wellbeing.

(b)protection from harm and neglect.

(c)education, training and recreation.

(d)the contribution made by them to society.

(e)social and economic wellbeing.

Care Act 2014, Section 1

Duty on Local Authorities to promote an individual's wellbeing including:
(a)personal dignity (including treatment of the individual with respect).

(b)physical and mental health and emotional wellbeing.

(c)protection from abuse and neglect.

(d)control by the individual over day-to-day life (including over care and support, or support, provided to the individual and the way in which it is provided).

(e)participation in work, education, training or recreation.

(f)social and economic wellbeing.

(g)domestic, family, and personal relationships.

(h)suitability of living accommodation.

(i)the individual's contribution to society.

The effective and timely sharing of information between agencies and organisations is essential to enable early intervention and preventative work for safeguarding and promoting welfare of those experiencing and at risk of abuse and harm. For this reason, this template Tier 1 Data Sharing Agreement is intended to apply to all areas of children's safeguarding. In the context of this document a Tier 1 Data Sharing Agreement can be understood as a strategic agreement between safeguarding partners defining the appropriate arrangements to support multi-organisational information sharing for safeguarding reasons, see Appendix 1 for further details.

The UK GDPR sets out seven key principles to comply with when processing personal data:

- Lawfulness, fairness, and transparency
- Purpose limitation

- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Please visit the ICO website for more detail on the principles.

Administration

The organisations below are signatories to this Tier 1 Data Sharing Agreement (see Appendix 5 for further details):

Table 1: Organisations

Organisation(s):
(Add rows as required)

Table 2: General signatories

Date Tier 1 DSA comes into force:	XX/XX/20XX
Last review:	XX/XX/20XX
Date for review of DSA:	XX/XX/20XX
DSA Owner (Organisation):	Organisation name
DSA Author(s):	Name

Table 3: Version control

Version	**Date**	**Author**	**Edit/Update**
V0.1 Draft	XX/XX/20XX	Name	First draft for consideration

Scope

This Tier 1 Data Sharing Agreement applies to organisations operating within *[add the relevant geographical area]*. It is a multi-agency Tier 1 Data Sharing Agreement between Local Authorities, NHS Trusts, Police, Probation and Prison Service. *[delete/add as relevant]*. A full list of signatory organisations can be found under section 3 Administration and in Appendix 5. The Tier 1 Data Sharing Agreement covers the operation of s16LA: the sharing of information about a child, or any other individual connected to a child, whether an adult or another child, where it is relevant to safeguarding and promoting the welfare of that child.

[Describe the Safeguarding Children Partnership and why it is relevant (Children Act 2004, Working Together Chapter 3, joined up responsibility of statutory partners leading on the arrangements to work together, function of non-statutory partners (signatories also to the DSA and significant role when safeguarding children, add governance structure etc.)]

This template is for use by professionals, staff and volunteers of organisations who have signed, and therefore agreed to the terms of this Tier 1 Data Sharing Agreement and providers of services commissioned by the organisations who have signed this Tier 1 Data Sharing Agreement. Safeguarding is everyone's responsibility, not just safeguarding practitioners.

The Care Quality Commission (CQC) describes safeguarding as protecting people's health, wellbeing, and human rights, and enabling them to live free from harm, abuse, and neglect. It is fundamental to high-quality health and social care.

The Department for Health and Social Care provides guidance on the Care Act 2014 through the 'Care and support statutory guidance' and describes adult safeguarding as 'an adult's right to live in safety, free from abuse and neglect. It is about people and organisations working together to prevent and stop both the risk and experience of abuse or neglect.'

The Care Act 2014 states that safeguarding duties apply to an adult aged over 18 who:
d) has needs for care and support (whether or not the authority is meeting any of those needs) and;
e) is experiencing, or is at risk of, abuse or neglect, and
f) as a result of those needs is unable to protect himself or herself against the abuse or neglect or the risk of it.

The Department for Education defines children's safeguarding as follows within their 'Working Together to Safeguard Children' guide to inter-agency working to safeguard and promote the welfare of children:

a. Protecting children from maltreatment
b. Preventing impairment of children's mental and physical health or development
c. Ensuring that children are growing up in circumstances consistent with the provision of safe and effective care
d. Taking action to enable all children to have the best outcomes

The Information Commissioners Office (ICO), and future Information Commission, recognises in their 10-step guide to sharing information to safeguard children that there is no single definition of safeguarding but highlights the inclusion of

a. preventing harm
b. promoting the welfare of a child; and
c. identifying risk in order to prevent harm (especially helpful where the risk may not be obvious to a single person or organisation).

Safeguarding should therefore be seen as a protection of wellbeing (including physical, mental & emotional); a prevention of harm and reduction of risk through care and support requiring information sharing. This allows intervention in immediate situations demanding the safeguarding of children but also sharing for prevention and early intervention in both less immediate or high-risk situations.

Information sharing with non-statutory agencies e.g., charities is within the scope of this Tier 1 DSA. There are a number of charitable organisations that offer support and services. Such organisations are not created under statute and therefore do not have statutory powers, nor are they subject to the same duties particularly 16E and 16LA of the Children Act 2004; nevertheless, they are often able to offer help and assistance in the form of counselling, advice, support and guidance as well as referring individuals to other organisations and charities within their network.

Purpose and benefits

The purpose of this Tier 1 DSA is to facilitate the lawful sharing, use and security of all relevant data including personal and special category data in order to safeguard and promote the welfare of a child. This Tier 1 Data Sharing Agreement will function as the foundation to embed strong, effective multi-agency safeguarding arrangements that are responsive to local circumstances and engage the right people. Some of the information shared will be processed for law enforcement purposes in accordance with Part 3 of the Data Protection Act 2018. Signatories to this agreement must be engaged to work in a collaborative way to provide support and intervention as appropriate. This approach will provide flexibility to enable joint identification of, and response to, both existing and emerging needs, and to agree priorities to improve outcomes. This Tier 1 Data Sharing Agreement provides an overall framework for the secure sharing of information between the organisations (multi-agency working) that are parties to it with the intention of:

- Complying with statutory and regulatory obligations to safeguard and promote the welfare of children
- Collaborating, sharing, and co-owning the vision for how to achieve improved outcomes for children
- Challenging appropriately and holding safeguarding partners to account effectively
- Sharing information effectively
- Ensuring that shared learning is promoted and embedded through changes to practice

Anonymous data may be shared for some of these purposes, where the information has been processed so that individuals are no longer identifiable, which do not directly relate to safeguarding individuals, but will help improve overall service provision for children and young people. Anonymous data will also be used for:

- Managing risks, performance, service planning, and auditing
- Providing information and support in accessible ways to help people understand the different types of abuse, how to stay safe and what to do to raise a concern about safeguarding and promoting the welfare of a child
- Raising public awareness so that communities as a whole, alongside professionals, play their part in preventing, identifying, and responding to abuse and neglect and promoting the welfare of children

Responsibilities and partner commitments

By becoming a partner to this Tier 1 Data Sharing Agreement, all organisations are making the following commitments. It is understood that signatories to this Tier 1 Data Sharing Agreement are committing their entire organisation to wholly support the principles and carry out their responsibilities to the full extent.

Table 4: Area of responsibility

Area of responsibility:
The parties to this DSA are committed to ensuring that information is shared appropriately for the purposes of safeguarding and promoting the welfare of a child, between those professionals/organisations across [add geographical area] and who have a legitimate need for that information.
Organisations signed up to this Tier 1 Data Sharing Agreement commit to sharing confidential information in accordance with their legal, statutory, and common law duties and meet the requirements of any additional supporting guidance.
All organisations must have in place policies and procedures to meet the legal requirements for data protection, and which are consistent with this DSA. The existence of, and adherence to, such policies provide all organisations with confidence that data shared will be transferred, received, used, held and disposed of appropriately.
The Common Law Duty of Confidentiality (CLDoC) does not apply to information shared in compliance with the Information Sharing Duty, meaning consent is not required, in CLDoC terms, or the need to consider whether sharing is in the overriding public interest.
Where processing is likely to result in a high risk to the rights and freedoms of a natural person (as per UK GDPR, Article 35), a Data Protection Impact Assessment will need to be completed and shared with the relevant partners as appropriate.
This Tier 1 Data Sharing Agreement does not replace the need to conduct a Data Protection Impact Assessment of the information, or processes involved. Where high risk is identified and this cannot be mitigated, prior consultation with the ICO is required otherwise the processing cannot go ahead.
An individual’s personal information must be accurate and up to date and will only be disclosed where the purpose for which it has been agreed to share clearly requires that this is necessary.

Area of responsibility:
Where the Information Sharing Duty applies, organisations must share information with another in scope organisation, or the requestor, if it is considered that sharing may facilitate safeguarding or welfare. This includes help the recipient assess need, make a decision, provide support or take action to safeguard and promote the welfare of a child provided that sharing is not more detrimental than not sharing.
When disclosing information about an individual; organisations will clearly state whether the information being shared is fact, opinion, or a combination of the two.
Whilst consent is not required by the Information Sharing Duty and is not the only possible lawful basis under data protection law when sharing information under the Information Sharing Duty, effective engagement with children and families remains critically important, particularly where access to support or intervention will be consent based.
Building understanding and trust supports better outcomes and helps families to participate meaningfully in support and intervention. Practitioners should exercise professional judgement in deciding when and how to inform families, taking account of any risks that transparency itself may pose, including the risk of harm or intimidation. Decisions should be proportionate, clearly recorded, and focused on the best interests of the child.
All organisations agree to make reasonable efforts to ensure that recipients of personal information are kept informed of any changes to the information that they have received, so that records can be kept up to date.
Careful consideration will be given to the disclosure of information concerning a deceased person, and if necessary, further advice should be sought before such data is released.
All organisations will ensure that Subject Access Requests and other Individual Rights requests made to them are responded to in accordance with the requirements outlined in the UK GDPR and the Data Protection Act 2018.
All organisations agree that appropriate training will be given to staff so that they are aware of their responsibilities to ensure personal information is processed lawfully and securely.
All staff will be made aware that disclosure of personal information, which cannot be justified on legal or statutory grounds, whether inadvertently or intentionally, could be subject to disciplinary action and where appropriate, regulatory investigation or enforcement action.

Area of responsibility:
Organisations are responsible for putting into place effective procedures to address complaints relating to the disclosure of personal information.
Extreme care and careful consideration should be taken where the disclosure of information includes third party information and particularly personal data relating to witnesses, victims or complainants.
The person or persons to whom a request is made must comply with such a request in relation to a child death review or child safeguarding practice review and if they do not do so, the safeguarding partners may take legal action against them.
To fulfil their organisation's statutory obligations, practitioners must share information where the criteria of the Information Sharing Duty are considered to have been met and consider and respond to requests for information from other organisations and practitioners in line with the duty. If documentation is requested, and this is not deemed necessary and proportionate, consider providing the relevant information extracted from the document instead. Practitioners must only use information shared under this duty for the purposes of safeguarding and promoting the welfare of children unless required by another statutory obligation or common law duty. When further processing information for another purpose, identification of a different lawful basis under data protection, of relevance to that purpose, is likely required.
In line with established best practice, practitioners should provide acknowledgement and timely feedback to organisations and practitioners from whom they have received information, to inform them of receipt and any decisions taken as a result. Where safe, practicable and appropriate, practitioners should make parents/guardians aware of concerns about other individuals in a child's life where it is relevant to the child's safety and welfare.

These responsibilities reflect, and should be read consistently with, relevant Information Commissioner's Office (ICO) guidance on data protection and information sharing, including the ICO's 10 step guide to sharing information to safeguard children and Data sharing: a code of practice. Partners commit to applying this guidance when interpreting and implementing the commitments set out in this section.

Local Authorities have a duty under the Children Act 1989, Care Leavers (England) Regulations 2010 and the Care Act 2014 to ensure a safe transition from Children's to Adult Services. Where there are ongoing safeguarding concerns or support needs, and it is anticipated that on reaching 18 a young person is likely to require adult safeguarding support, the relevant arrangements should be discussed as part of the transition and appropriate information should be shared. For many children, once they turn 18, information will be retained by agencies in line with their usual retention periods. Some

young people, particularly those with special educational needs and disabilities or care leavers, may continue to receive support from organisations, although the information sharing duty will no longer apply. Organisations should therefore prepare for this transition accordingly, particularly where proxy access may be appropriate or where support will move to other organisations, such as adult services, who would benefit from early knowledge of individuals needs and their support packages in order to ensure continuity of support and prompt assessments.

Lawfulness

Partners agree that in order to share personal data, there needs to be a relevant legal gateway. It is important to note that the existence of this Tier 1 Data Sharing Agreement does not provide partners with a legal gateway or secure an automatic right or obligation to share information with or from another partner. This may come from statute, common law, or legal precedence. Statutory powers (also referred to as legal gateways) will differ between the signatory organisations and cannot be prescribed in this Tier 1 Data Sharing Agreement. A list of commonly used legal gateways / applicable legislation for safeguarding sharing can be found in Appendix 3. For the purposes of this document, the term “processing of personal data” has the same meaning as, and is defined by, the Data Protection Act 2018.

Principal law and legislation governing the protection and use of personal information is:

a. UK General Data Protection Regulation (UK GDPR)

b. Data Protection Act (DPA) 2018

c. Human Rights Act 1998 (article 8)

d. The Common Law Duty of Confidentiality

e. Data (Use and Access) Act 2025

The signatories of this Tier 1 Data Sharing Agreement understand that Consent is one lawful basis, but it is not required by the Information Sharing Duty when sharing information and it is highly unlikely to be an appropriate choice of lawful basis in relation to the Information Sharing Duty or other sharing for safeguarding and promoting welfare purposes. This is because there is often an imbalance of power between the parties, so consent might not be freely given, and because consent might later be withdrawn.

Crucially, in cases of suspected maltreatment, exploitation, abuse or neglect, seeking consent from the suspected perpetrator, or another person connected, is likely to undermine prospective safeguarding efforts and may increase risk of harm. In most safeguarding scenarios you will be able to find a more appropriate lawful basis. The most common lawful basis suitable for safeguarding are public task, legitimate interests, and legal obligation. The UK GDPR provides several bases for sharing personal information. 10 step guide to sharing information to safeguard children). The UK GDPR provides several bases for sharing personal information.

Trusting relationships with children and families are central to effective safeguarding and support. Where it is safe and appropriate, practitioners should be open and transparent about information sharing, helping children and parents/carers understand why information is shared and how it will be used.

The difference between consent to treatment/service opt-in and consent to share information under data protection laws must be understood by all partners to this Tier 1 Data Sharing Agreement. If consent to share information is considered to be required, this must be escalated to the relevant partner organisation's DPO for review. The police usually process personal data for law endorsement purposes, but local authorities do in some circumstances. Your DPO will provide advice on when this applies to your activities. If the DSA includes processing for law enforcement purposes, then you must list the relevant parties and their purposes in the table.

Guidance

Partners will rely on the following guidance to adhere to principles defined in this Tier 1 Data Sharing Agreement.

National Guidance:

Children:

- Working together to safeguard children (Department for Education)
- Information sharing advice for safeguarding practitioners (Department for Education)
- 10 step guide to sharing information to safeguard children (Information Commissioners Office)
- Data sharing: a code of practice (Information Commissioners Office)
- *[Add ISD guidance link to replace the above non statutory information sharing guidance link]*

Local Guidance:

- XX
- XX

[add joint regional safeguarding children policies/procedures/ToR or other as relevant]

Security standards

Each partner will be responsible for ensuring data is subject to sufficient security.

All partners signed up to this Tier 1 Data Sharing Agreement must ensure that appropriate organisational and technical policies and procedures are in place to protect the security of personal data shared under this Tier 1 Data Sharing Agreement. These measures must be designed and implemented in line with UK data protection legislation and relevant ICO guidance, including the principles of data protection by design and by default.

Partners must ensure that personal data is protected against unauthorised or unlawful processing, accidental loss, destruction or damage, by implementing proportionate and risk based security controls, taking account of the nature, scope, context and purposes of the processing and the risks to individuals, particularly to children and other vulnerable persons.

All reasonable steps should be taken to ensure that confidentiality of data is maintained, the integrity of data is preserved, and that data remains available where needed. Controllers must also consider determining how they will test/audit the effectiveness of information security controls as part of a Data Protection Impact Assessment.

Sharing arrangements involving shared systems/assets will require joint decisions on security controls, therefore responsibility may be shared (pertinent to joint controller arrangements). This may include (but is not limited to) decisions on:

- A satisfactory level of compliance with industry cyber/information security standards (e.g. Cyber Essentials)
- A role-based access model
- Patching schedules
- Remote access solutions
- Third party security assurances and contractual arrangements (which may permit certain autonomy to maintain security)
- Recovery point/time objectives

It may be applicable to complete a version of the Data Security and Protection Toolkit where there are different versions depending on the size and type of organisation. The Data Security and Protection Toolkit is something which will be relevant for health care organisations and local authorities; however, the police have their own standards they adhere to. Organisations should work towards an equivalent standard depending on the type of organisation and the level of data being processed.

A system level security policy should be developed jointly for such assets to document the agreed security controls/assurances for the sharing partners and demonstrate controller responsibility.

Appropriate contractual, data processing and confidentiality agreements must be in place to underpin the processing of personal information by a third party / processor.

- What are ‘controllers’ and ‘processors’? | ICO
- Contracts and liabilities between controllers and processors | ICO

Proportionality and necessity

The data relevant under this Tier 1 Data Sharing Agreement may include personal data, special category data (including confidential patient information such as health and social care records), and criminal offence data. Confidential patient information is information given in confidence relating to an individual's health or care and must be handled in accordance with data protection legislation and, where applicable, the common law duty of confidentiality. Such data may be shared where it is necessary and proportionate for the purposes of safeguarding and promoting the welfare of a child.

Partners agree that only information that is relevant to the purposes should be shared with those partners who need it (need to know basis). Assessing proportionality and necessity for any sharing initiative under this Tier 1 Data Sharing Agreement is paramount and should be documented to assure compliance with current UK data protection legislation. Where data is shared for the purposes of safeguarding and promoting the welfare of a child, both the benefits and the risks must be balanced against each other to assure the right of proportionality and necessity. Organisations signed up to this Tier 1 Data Sharing Agreement must therefore include Caldicott Guardians (for Health), Service Leads or other equivalent individuals as they must be core to such decision-making. Data minimisation and proportionality will be maintained by only asking for data that is needed to fulfil a specified purpose.

Partners must consider any harm or detriment that may come from sharing information and make sure this does not outweigh what is trying to be achieved (including least intrusive amount of personal information to be shared appropriate to the risk presented). This is particularly important for special category data. Partners will consider who could be affected by any disclosures, given that sharing information about one individual may also have an effect on the privacy rights of others. Information must be of the right quality to ensure that it can be understood and relied upon.

Organisations will ensure they have verified that they are each referring to the same child/individuals before sharing information.

Retention

Records will be retained and disposed of in accordance with data protection legislation and national and local/organisational guidelines. Each organisation which has received information referred to in this Tier 1 Data Sharing Agreement has to follow their own Retention and Disposal Policy which should state how long they will keep different types of information. Additionally, organisations should consider the business need beyond any national/industry code or guidance which could justify a shorter or longer retention period. Retention periods should be agreed with sharing partners, at the early stages of data sharing, especially sharing arrangements involving shared systems/assets require joint decisions on retention and/or system configuration as they are more complex.

Health and Social Care partners will consider the Records Management Code of Practice for Health and Social Care to inform decision making. Other partners will consult the relevant industry guidelines.

National inquiries must be considered when assessing records for destruction.

Information shared under this Tier 1 Data Sharing Agreement will be managed throughout its lifecycle in accordance with UK data protection legislation and each partner's retention and disposal policies, including being held securely, used only for agreed purposes, and retained only for as long as necessary and lawful; where a sharing activity ends, or where this Tier 1 Data Sharing Agreement expires or is terminated, partners will ensure that information is securely deleted, destroyed, anonymised, or retained under a separate lawful basis as appropriate, and that no further processing takes place under this Tier 1 Data Sharing Agreement once it has ended.

Individuals whose personal data is processed for law enforcement purposes have the rights set out in, and subject to the provisions of, Part 3 of the Data Protection Act 2018.

Individuals Rights

The partners agree that in simple sharing arrangements each Controller will handle subject rights requests in accordance with applicable data protection legislation and their own established processes and policies. Requests relating to information shared for safeguarding purposes are likely to require careful consideration and may require assistance from partners as the provider of the information may be aware of a wider context to make a fully informed decision. Therefore, sharing partners agree to set out clear arrangements for the handling of individual's rights and provide reasonable assistance to sharing partners as required.

The right to be informed – Partners must ensure that individuals are informed about the collection and use of their personal data and are provided with the privacy information required as per current data protection law. See the following section 'Transparency' for further detail.

The right of access – Sharing partners will set out clear responsibilities, including (but not limited to); whether there will be a central process to manage and co-ordinate requests, what the process shall be if a request is received by them but is relevant to another organisation, how partners' involvement affects what they should disclose and the process for determining lawful reasons to withhold data from disclosure (i.e. if they are viewing data in a shared asset but are not controller nor a joint controller of the data, or if they are a joint controller).

The right to object and the right to restrict – Sharing partners will set out clear responsibilities, including (but not limited to); whether there will be a central process to manage and co-ordinate objections and restriction requests, what the process shall be if an objection or restriction request is received by them but is relevant to another organisation and the process for determining whether to uphold the objection or restriction request (although unlikely due to the nature of processing).

The right to rectification – Sharing partners will agree a process of how to respond to requests for rectification (i.e. if received by them but it is relevant to another organisation). The process will be dependent upon the sharing arrangement; this may require action from multiple partners (especially when a request for rectification of a professional opinion is received) or by a single partner that has provided the data into a shared asset and may require partners to assist each other to determine whether data should be rectified.

The right to erasure - Sharing partners will agree a process of how to respond to requests for erasure (i.e. if received by them but it is relevant to another organisation). It is unlikely to uphold a request for erasure when processing for safeguarding reasons.

Automated decision-making and profiling – If the sharing arrangement is to involve automated decision-making or profiling then the sharing partners will agree how individuals affected will be informed of this (unless an exemption applies) and how requests for a member of staff to review any such activity will be handled. As it stands, data used for safeguarding purposes is unlikely to be classed as ‘automated decision making’ or ‘profiling’ without human intervention prior to decisions being made that affect individuals.

The right to data portability – If the sharing arrangement is to involve the processing of data based on the explicit consent of the data subject or a contract with the data subject (which are both highly unlikely for the purposes of safeguarding), or data will be carried out by automated means, then the sharing partners shall ensure that it is possible for data to be provided to the data subject in a structured, commonly used and machine-readable format and/or have this data transmitted to another controller. The lawful basis of processing data for safeguarding purposes is not likely to be explicit consent. Therefore, it is unlikely that the right to data portability applies.

Any Information Rights request directed at [add name of partnership] should be forwarded to [add relevant details] to coordinate the appropriate response. When a partner agency requires cooperation from the Partnership to respond to a Subject Access Request, they should contact the relevant Business Support Team Manager to ensure appropriate liaison with the [add relevant details].

Transparency

Each organisation must be clear, open and transparent with data subjects about the collection and use of their personal information, paying particular attention to the 'right to be informed'. The sharing partners (controllers) each have a responsibility to take reasonable steps to ensure that individuals (to whom data they are processing pertains) are informed of the uses of their data. The sharing partners will therefore agree an approach to informing individuals about the sharing of information for the purposes of safeguarding and promoting the welfare of a child. This may, for example, take the form of each partner updating their own privacy information (i.e., a website privacy notice) or the partners may agree to reference a single privacy notice from their own privacy information, which is then maintained by one or several organisations (e.g., joint controllers). The privacy information must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language, tailored to children if required.

Best practice in respect of transparency is to adopt a layered approach to communicating how individuals' data is used (for example through privacy notices, written materials, or conversations). However, given the nature of information sharing for safeguarding and promoting the welfare of a child, it will not always be appropriate or safe to provide full transparency. In such cases, sharing partners must consider and apply the relevant exemptions under Part 2 of the Data Protection Act 2018, including where providing information would be likely to cause serious harm. Where processing is carried out for a law enforcement purpose under Part 3 of the Data Protection Act 2018, the separate transparency requirements and exemptions under that regime apply.

Staff training, development, supervision and management

Each sharing partner must ensure that its staff and contractors are sufficiently trained to handle personal data appropriately as part of their controller responsibilities under UK data protection law (the UK GDPR principle of 'accountability' and specifically principle 5(f) (integrity and confidentiality (security)) as an appropriate organisational measure). This should include training on confidentiality, data protection, record keeping, records management, system training, as well as more specific training on handling individuals' rights requests for those staff typically involved in these, etc. Sharing partners should therefore consider whether staff affected by a new sharing arrangement will require additional training (in addition, controllers should continually assess the training needs of their workforce, which is often done by maintaining/appraising a 'Training Need Analysis' on a routine basis).

All staff must have access to their organisation's relevant policies, this Tier 1 Data Sharing Agreement, and any jointly developed materials. Only staff who are authorised and have a legitimate need to know must be permitted to access information, or particular types of personal data, and access must be role based and proportionate to their responsibilities. All authorised staff must receive appropriate training on data protection and safeguarding information sharing, including the risks and consequences of inappropriate disclosure. Access to information must be managed and enforced through appropriate organisational and technical measures, including role based access controls, supervision, audit, and monitoring. Staff contracts must include confidentiality clauses, and each organisation must have disciplinary procedures in place to address unauthorised or inappropriate disclosures.

The process of supervision is generally confidential between the supervisor and supervisee(s). The ground rules in relation to confidentiality will be made explicit, such as ownership of supervision records, retention of information. There may be occasions when it is necessary to share information with other practitioners/ managers/ external agencies/professional bodies in the best interests of the child at risk in line with organisational and multi-organisational information sharing agreements. Poor or dangerous practice will be addressed in line with partner organisation policy and procedures.

The partners of this Tier 1 Data Sharing Agreement will work together to jointly develop staff training materials to allow organisations to this Tier 1 Data Sharing Agreement to incorporate the principles of this Tier 1 Data Sharing Agreement. Resources can be found in Appendix 4.

Incident management and complaints

Incidents involving information and data must be treated with priority and urgency. This includes, but is not limited to, actual or suspected personal data breaches, loss or unauthorised disclosure of information, unauthorised access to systems or records, and incidents that may compromise the confidentiality, integrity, or availability of information shared under this Tier 1 Data Sharing Agreement. Swift action should be taken to contain incidents and prevent both the number of individuals that may be affected and increased severity for those already affected. As such, sharing partners must inform the responsible controller as soon as possible (where they become aware of an incident that they are not responsible for or are only partially responsible for). Sharing partners must also determine whether other sharing partners (beyond those responsible) should be informed as concerns may have been, or be, raised to them that are linked to the incident, which they may otherwise not know.

Given the nature of the data involved in processing for safeguarding purposes, care and consideration should be given to who needs to be informed of an incident (in terms of both sharing partners, as well as the individuals affected and/or third parties). It is important to note that certain personal data breaches must be reported to the ICO within 72 hours.

Where an incident is isolated and deemed to only affect one sharing partner than the incident may be handled solely by that sharing partner according to their own incident management policy and processes. Where multiple sharing partners are affected, they must be prepared to establish a joint incident response plan. Clear responsibilities should be set out for any joint controller arrangements.

Complaint handling should follow a similar path; however, they are unlikely to require such priority/urgency unless they are intrinsically linked to an incident.

All partner organisations must put in place processes that allow concerns about non-compliance with this Tier 1 Data Sharing agreement to be reported to the designated person.

Common sharing initiatives and areas of work

The information that is being shared needs to flow to all parts of the system, with different parts of the system having different requirements, often with data being shared via different routes. The below sharing initiatives are covered by this Tier 1 Data Sharing Agreement and give detail of how data should be shared under each initiative, and how it is being used to safeguard children and their families.

Table 5: Data sharing initiatives

Child Death Reviews - Children
[Describe the relevant common sharing initiatives / areas of work]
Child Death Overview Panel (CDOP) - Children
[Describe the relevant common sharing initiatives / areas of work]
Child Safeguarding Practice Reviews
[Describe the relevant common sharing initiatives / areas of work]
Child Protection Notifications
[Describe the relevant common sharing initiatives / areas of work]
Family Help
[Describe the relevant common sharing initiatives / areas of work]
Multi-Agency Child Protection Team (MACPT)
[Describe the relevant common sharing initiatives / areas of work]
Multi Agency Public Protection Arrangements (MAPPA) – Children and Adults
[Describe the relevant common sharing initiatives / areas of work]
Multi Agency Risk Assessment Conference (MARAC) – Children and Adults
[Describe the relevant common sharing initiatives / areas of work]
Multi Agency Safeguarding Hub (MASH) – Children and Adults
[Describe the relevant common sharing initiatives / areas of work]

Prevent – Children and Adults
[Describe the relevant common sharing initiatives / areas of work]
Risk Outside the home – Children and Adults
[Describe the relevant common sharing initiatives / areas of work]
Section 20 (Children Act 1989)
[Describe the relevant common sharing initiatives / areas of work]
Section 47 (Children Act 1989)
[Describe the relevant common sharing initiatives / areas of work]

[Add or remove rows as required]

It should be noted that the above list is not exhaustive but any data sharing for Safeguarding Children purposes will still fall under this Tier 1 Data Sharing Agreement.

Dissemination, monitoring and review of the agreement

This protocol will be shared with all signatories, processors and relevant parties for the purpose of upholding the principles of this Tier 1 Data Sharing Agreement.

It is intended that this Tier 1 Data Sharing Agreement contains high level principles and partner commitments only. It will therefore be reviewed every [add number of years] to establish if the sharing remains necessary, sill operates as intended and, has or is, achieving the intended benefits, unless legislative changes or other significant changes require immediate action. The monitoring and review of this protocol will be undertaken by [add organisation, group or other as relevant].

Subject to there being no significant changes, the Tier 1 Data Sharing Agreement may be extended by a further [add number of years] without seeking further approval or new signatures. However, any significant changes will require the full approval process.

In the event that this Tier 1 Data Sharing Agreement is not renewed or is otherwise withdrawn, it is incumbent on the parties to amend their records accordingly and to communicate the status of the Tier 1 Data Sharing Agreement within their respective organisations, to interested parties and the wider public as necessary. The obligations of confidentiality imposed on the Parties by this Tier 1 Data Sharing Agreement shall continue in full force and effect after the expiry or termination of this Tier 1 Data Sharing Agreement.

Signatories

If this Tier 1 Data Sharing Agreement is published to a system that manages signatures/agreement, then this section can be removed.

Each organisation should identify who is the most appropriate post holder within their agency to sign the DSA having taken account of their organisational policy and the fact that the signatory must have delegated responsibility to commit their agency/organisation to the Tier 1 Data Sharing Agreement. Additionally, each agency will be asked to identify the post which is responsible on a day-to-day basis for monitoring compliance with this Tier 1 Data Sharing Agreement.

By signing this Tier 1 Data Sharing Agreement, all signatories acknowledge and accept the requirements placed upon them and others within their organisations by the DSA and their responsibilities under data protection legislation. Decision needs to be made if the signatory is a list of organisations all signing one document in turn, or if a single organisational signature is collected per copy of the DSA, with a central point of collection and maintained list of signatories.

Table 6: Signatories - Local Authority

1. Signed on behalf of a Local Authority
Name:
Role:
Signature:
Date signed:
Person which is responsible on a day-to-day basis for monitoring compliance with this DSA:

Table 7: Signatories - ICB

2. Signed on behalf of Integrated Care Board (ICB)
Name:
Role:
Signature:
Date signed:

Person which is responsible on a day-to-day basis for monitoring compliance with this DSA:

Table 8: Signatories - Chief of Police

3. Signed on behalf of Chief of Police
Name:
Role:
Signature:
Date signed:
Person which is responsible on a day-to-day basis for monitoring compliance with this DSA:

Table 9: Signatories - Extra

4. Signed on behalf of
Name:
Role:
Signature:
Date signed:
Person which is responsible on a day-to-day basis for monitoring compliance with this DSA:

[Add or remove rows as required]

Appendix 1 – Glossary of terms

Table 10: Glossary of terms

Term	Definition
Ad-hoc data sharing	Information sharing outside a formal meeting or system, often on a one-off basis.
Appropriate Policy Document (APD)	An appropriate policy document is a short document outlining your compliance measures and retention policies. It is required under the Data Protection Act 2018 for some of the conditions documented in Schedule 1 (Part 1, 2 and 3).
Caldicott Guardian	A senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly. All NHS organisations and local authorities which provide social services must have a Caldicott Guardian. Further, guidance has been issued under the Health and Social Care (National Data Guardian) Act 2018 that recommends "other organisations providing services as part of the publicly funded health service, adult social care, or adult carer support" should have a Caldicott Guardian by 30/06/2023:
Common law duty of confidentiality	The common law duty of confidentiality is not codified; it is based on previous judgements in court. Whilst various interpretations of the common law may be possible it is widely accepted that, where information which identifies individual service users is provided and held in confidence, the three key ways that disclosure may be justified are: 1. the service user has given consent for their information to be used; 2. the balance of public and private

	interest favours public interest disclosure; or 3. a statutory basis exists which permits or requires disclosure. (source: Health and Social Care (Control of Data Processing) Act (Northern Ireland) 2016, Explanatory Note, Common Law Duty of Confidentiality) The Information Sharing Duty creates a legal requirement to share information relevant to safeguarding and promoting the welfare of a child, reducing uncertainty and negating the need to determine overriding public interest or seek consent. Confidential information, including health information, can be shared without consent for the purposes of safeguarding and promoting welfare, provided the criteria in s16LA of The Children Act 2004 and data protection requirements are met. This applies to information about the child, alongside information about any other individual connected to a child, provided it is relevant to the child's safety and welfare. Organisations and practitioners may also request confidential information from other organisations – requests must include enough contextual information for the recipient to determine if the information sharing duty applies to be confident sharing, and decide what information is appropriate to share. Where risk to the child, or need, is less obvious and practitioners are hesitant to share special category data, they may wish to ask for additional information from the requestor or request additional information about the child from other organisations and practitioners to better determine the significance of the information they are considering sharing.

Consent	Consent under data protection law is defined as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. Under data protection law practitioners do not need to obtain consent from children and families to share information relevant to safeguarding and promoting the welfare of a child as they should be operating under an alternative lawful basis, such as legal obligation or public task.
Criminal Offence Data	Includes personal data relating to the alleged commission of offences by the data subject, or proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.
Data	The use of data in this document must be understood as information which may refer to non-identifiable or identifiable data. It will be specified if it refers to personal data.
Child	Anyone who has not yet reached their 18th birthday. The fact that a child has reached 16 years of age, is living independently or is in further education, is a member of the armed forces, is in hospital or in custody in the secure estate, does not change their status or entitlements to services or protection.
Data Controller / Joint Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the

	purposes and means of the processing of personal data.
Data Protection Act (DPA) 2018	The DPA 2018 sits alongside and supplements the UK GDPR.
Data Protection Impact Assessment (DPIA)	A process to help you identify and minimise the data protection risks related to processing of personal data. A DPIA is legally required in some circumstances.
Data Protection Officer (DPO)	The primary role of the data protection officer (DPO) is to ensure that their organisation processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules.
Data Subject	The individual to whom the data being processed relates and is identified/identifiable by that data.
Data Sharing	Data sharing as used within this document can be understood as sharing of personal data.
Data Sharing Agreement (DSA)	Terminology can vary (Data Sharing Protocol, Data Sharing Contract, Personal Data Sharing Agreement) but can be used interchangeably in the guidance. A DSA can be used between sharing partners (Controllers) to help demonstrate compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the common law duty of confidentiality and other relevant laws. It should help you justify your data sharing, clarify responsibilities of the sharing partners and set agreed parameters for the use of data.
European Economic Area (EEA)	The EEA includes EU countries and Iceland, Liechtenstein, and Norway. The UK has adequacy regulations in place

	about these countries (expected to last until 27 June 2025).
Information	The use of information in this document must be understood as organised data providing context which may refer to non-identifiable or identifiable data. It will be specified if it refers to personal data.
Information Commissioner's Office (ICO), which in future will be known as the Information Commission	The UK's independent body set up to uphold information rights.
Law Enforcement Processing	Processing (including sharing) of personal data by competent authorities (for definition click here) for a Law Enforcement Purpose.
Law Enforcement Purposes	As defined by Section 31 Data Protection Act 2018 - the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (for details click here).
Legal gateway	Legislation and common law that establishes justifiable grounds for the processing of personal data.
Local Authority (LA)	An LA is a local government organisation responsible for the administration of government policy at a local level.
Means [of processing]	Actions taken in the processing of data to achieve the purpose(s) for its processing i.e. how the data is processed but can also be considered to extend to what data is used to achieve the purpose(s).
Multi-Agency Safeguarding Hub (MASH)	The Multi-Agency Safeguarding Hub (MASH) brings key professionals together to facilitate early, better quality information sharing, analysis, and decision-making, to

	safeguard vulnerable children more effectively.
Organisations and practitioners	This means those to whom s16LA (4) applies. It is the organisation that is bound by the statutory Information Sharing Duty – in legislation, these organisations, and the practitioners working on their behalf, are referred to as relevant persons.
Personal data	Data that relates to a living identified or identifiable individual.
Processor	A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.
Purpose(s) [of processing]	Reasons to process personal data.
Recipient	Another organisation or practitioner within s16LA (4) with whom information is shared.
Requestor	An organisation or practitioner within s16LA (4) who requests information from another organisation or practitioner to whom the duty applies.
Relevant functions	Functions of the organisation receiving the information relating to safeguarding and promoting the welfare of a child, including their capacity to assess need.
Safeguarding and promoting welfare	This term is used across children's social care legislation and should be considered to encompass identifying need in order to prevent harm or escalation of needs, promoting the welfare of a child as well as protecting from harm. The ICO 10 step guide to sharing information to safeguard children illustrates what kinds of information should be considered relevant, with Working together to safeguard children 2026 providing a definition of

	safeguarding and promoting welfare of children.
Secure File Transfer Protocol (SFTP)	A protocol for securely accessing and transferring large files across the web.
Special Category Data	Data pertaining to an identified or identifiable individual that reveals their racial or ethnic origin, political opinions, religious or philosophical beliefs, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
Tier 1 DSA	In this document a Tier 1 Data Sharing Agreement can be understood as a Multi-Agency Safeguarding Data Sharing Agreement which can be used by all agencies and organisations within the relevant geographical area to provide a framework for data sharing between the partners. Sometimes a Tier 1 Data Sharing Agreement is referred to as: Data Sharing Protocol, Data Sharing Charter, and others.
UK Data Protection Legislation	For the purpose of this template/guidance the UK data protection legislation means the UK GDPR and the DPA 2018 and regulations made under the DPA 2018 which apply to a party relating to the use of personal data.
UK General Data Protection Regulation (GDPR)	Legislation that determines lawful and unlawful use of individuals' data, and places requirements on those processing data, to ensure appropriate use and adequate protections. It should be read alongside the DPA 2018.

Appendix 2 – Information sharing checklist

By sharing information for the purposes of safeguarding and promoting the welfare of a child, we work better together, and this Tier 1 Data Sharing Agreement [add name of DSA] encourages the appropriate sharing of information between the relevant agencies. If you cannot identify from the information you are planning to share, then you are free to share. However, if the information identifies someone, please use this checklist to help you determine that it is safe to share information. Here is a simple flow chart of what you will need to do to go from having concerns about sharing data to sharing data legally and securely with confidence.

Prior to engaging in any form of sharing, it is appropriate to seek support from the IG Team or safeguarding lead. Where necessary it might be deemed appropriate to complete a Data Protection Impact Assessment prior to any sharing of information.

Why is the information needed?

What is the purpose for sharing the relevant information, think about the purpose for individuals, your organisation and the wider public.

What information is needed?

Be specific and descriptive, consider how often it is required? Refer to the data item template available under 5. ‘Information to be shared by partners’ within the guidance document.

What organisation can provide the information?

Have you explored if the information is available already in other parts of your organisation. Have you spoken to a counterpart in the potential sharing organisation who can advise you on what information is available and how often?

Have you completed a Data Protection Impact Assessment (DPIA)?

Be aware that a DPIA is likely to be a legal requirement. Complete it before you start processing any data. Use the guidance document to learn more about the requirement to complete a DPIA.

How will it be transferred?

Consider your options and assess the risk of those. Transfers must be safe and secure, consult with your technical teams for more complex digital solutions (e.g., data transfer system to system or via Secure File Transfer Protocol [SFTP]).

Where will it be held?

Consider your options and assess the risk of those. Any information must be held safe and secure, consult with your technical teams for more complex digital solutions.

Are you sure the information is accurate and not misleading?

Take all reasonable steps to ensure the personal data you hold is not incorrect or misleading. If you discover that personal data is incorrect or misleading, you must take steps to correct or erase it as soon as possible. Carefully consider any challenges to the accuracy of personal data.

How will you process it?

Define what solutions are available to process the information (e.g., data warehouse, modelling, risk scoring, manual usage to inform cases), work closely with the relevant teams (e.g., security, analytics, IT, ethics).

How long will you keep it?

Follow your internal retention policy and establish how long you need the information. Include any potential outcome products and long-term requirements to hold the data.

How will you delete the data?

Follow your internal records retention or data destruction policy to assure safe destruction of the information you hold. Consider the method depending on your storage solution to allow for safety of destruction.

Ad-hoc Information sharing checklist (e.g. sharing ad-hoc for example during 'corridor conversations')

Why is the information needed?

What is the purpose for sharing the relevant information? Think about the purpose for individuals, your organisation and the wider public.

What information is needed?

Be specific and descriptive, consider what information is necessary and relevant.

Is it fair to share in this way?

Consider less intrusive ways of fulfilling your purpose or reach your objectives and consider what individuals are expecting to happen to their data.

What are the benefits and what are the risks?

Balance the benefits for an individual and/or individuals whose data will be affected against the risks of harm it could cause.

Where does the information originate from, does the source organisation need to be consulted?

Consider who is best placed to assess disclosure decisions around the risk of causing harm (e.g. interference with a police investigation, disclosure of details not knows to the recipient (adopted child).

What needs to be done to transfer the information securely?

What technical and organisational measures are appropriate to ensure the security of the data.

Am I being transparent about information sharing?

Consider what you have to tell people about sharing their data and how you will communicate that information in a way that is concise, transparent, easily accessible and uses clear and plain language.

Check your organisational policies and procedures

What policies and processes around sharing are in place and what guidance must be considered.

Ask for help to make disclosure decisions

Consult colleagues, managers and Caldicott Guardians if you are unsure about sharing information.

Document your decision

Document your decision as appropriate.

Appendix 3 – Applicable legislation

[Link to any locally held list of applicable legislation here]

Appendix 4 – Joint resources

Table 11: Joint resources

Name of document/tool	Description	Source organisation(s)
e.g. Training material, fair processing notices, DSA & DPIA templates, policies, guidance etc.	*e.g. Lawful Basis and Legal Framework document agreed by all statutory partners and shared with all non-statutory partners.*	*e.g. the content has been produced by the Police, Health Trust and the Local Authority, input from Barnardo's has been received and included.*

[Add or remove rows as required]

Appendix 5 – Partners to this agreement

Table 12: Partners to this agreement

Organisation	Address	ICO registration number	Name of contact	Contact details

[Add or remove rows as required]

UK Government

About this publication:

enquiries www.gov.uk/contact-dfe
download www.gov.uk/government/publications

Follow us on X: @educationgovuk
Connect with us on Facebook: facebook.com/educationgovuk