



Data Sharing Agreement

(including agreement for use of Transform Data View)

between

Somerset County Council

and

**Settings, Academies and
other Education Providers**

2022-23

Authors:

Amy Brittan (SSE DPO Schools)

Rebecca Martin (SCC Information Governance)

Dan Western (SCC Application Support Team)

Tina Bacon (SSE MIS Service)

Ellie Dalwood (SSE Schools Information Support Manager)

Consulted: Sandra Verrier (Central Data Team)

Date of agreement: 27/07/22

Proposed Review Date: July 2023 for Sept 2024

Names used:

Somerset County Council (the Local Authority) – the LA

Settings, Academies and other Education Providers – Education Providers

Contacts:

Information Governance: InformationGovernance@somerset.gov.uk

eLIM: dposchools@somerset.gov.uk

Central Data Team: coredatateam@somerset.gov.uk

Changes from 2021-22 document

5.3.2	Removed reference to educ email system
5.3.3	Removed reference to password protected documents; replaced with reference to using encryption tool when sending sensitive data
6.2	Reference to data from Capita One feeding into Transform Data View
8.2	Included reference to Transform Data View
Appendix C	Addition of Appendix C – Transform Data View information sharing agreement

Contents

1. What is a Data Sharing Agreement?	4
2. What are the LA Justifications for receiving pupil level data?	4
3. What data will be collected?	6
4. How will the data be used?	6
5. How will the data be transferred?	6
6. Will the data be shared with others?	8
7. What does the Education Provider agree to?	8
8. What does the LA agree to do?	10
9. Support from the LA.....	10
10. Data security breaches and reporting procedures	11
11. Appendix A - List of Data Items transferred between Education Providers and the LA (as of August 2020)	13
12. Appendix B – Data Description	14
13. Appendix C - Transform Data View Information Sharing Agreement ...	15

1. What is a Data Sharing Agreement?

- 1.1. This Data Sharing Agreement sets out the policies, procedures, roles and responsibilities of how parties will share personal data.
- 1.2. The introduction of the General Data Protection Regulation makes it a requirement for organisations that share personal data to have an agreement.
- 1.3. The main benefits of this agreement between the LA and Education Providers will be:
 - Meeting the requirements of the data protection laws and regulations and the ICO Code of Practice;
 - Reducing the administrative burden on Education Providers – as data will only be input once but used many times for the benefit of children and employees;
 - Providing better targeted services to all children and employees;
 - Ensuring the safety and wellbeing of individual children and employees;
 - Inclusion in the Overarching Information Sharing Protocols with the Avon and Somerset Police and the Local NHS CCG, Partnership and Trusts.
- 1.4. This agreement should be ratified and signed by the Education Provider by recording approval on the electronic form supplied each year. The LAs agreement is given by the provision of the agreement.
- 1.5. The data as to which Education Providers have signed up to the agreement will be provided to teams within the LA but not shared with other agencies unless covered by this agreement or by other statutory or legal requirements.
- 1.6. The LA will contact each Education Provider to inform them of the Agreement and may adjust the services it offers considering an Education Provider not signing the agreement.

2. What are the LA justifications for receiving pupil level data?

2.1. The LA has justifications for receiving pupil level data as detailed below:

2.2. DfE Admissions Codes

- 2.2.1. Education Providers are required to co-ordinate admissions with the LA at either First Time Admissions or Secondary Transfer stages. Regular submissions of student record updates to the LA are necessary to ensure that admissions process runs smoothly. This relates especially to the need for letters generated to parents to be based on accurate information and to ensure that accurate and up-to-date information is available when admissions decisions are

made to ensure that all pupils and families are treated as equitably as possible and that the relevant admissions policy and Education Providers Admissions Code of Practice are complied with.

2.3. Education Act 2002

2.3.1. Section 175 of this Act places a duty on both the Education Provider and the LA to safeguard and promote the welfare of children. The LA's ability to fulfil this role is dependent on ongoing receipt of core pupil data from Education Providers to ensure properly informed decisions are reached. Without this the LA would have to make decisions and allocate resources based on an incomplete pupil dataset. This would lead to inefficiencies and pose an obvious increased risk to vulnerable children and young people.

2.4. Education Act 1996

2.4.1. Section 436A imposes a duty on the LA to identify and monitor children missing education. This was further clarified by the DfE's guidance 'Children Missing in Education' (November 2013, updated September 2016). The LA's ability to perform its duties effectively is reliant on the regular transmission of electronic pupil updates from all Education Providers in Somerset.

2.4.2. Section 14 (1) requires the LA to conduct Educational Provision place planning. This is dependent on regular pupil updates being received from Education Providers. (However, Personal Identifiable data at individual level is not be used for planning purposes).

2.4.3. Section 444 places responsibilities on the LA in terms of enforcing pupil attendance. Electronic updates from the Education Providers about pupil attendance are required to support this.

2.5. Exclusions

2.5.1. Education Providers are obliged by its funding agreement to follow current law and DfE advice on Exclusions. Exclusions will be reported to the LA by the Education Provider electronically from the Educational Provider's MIS system.

2.6. Other Legislation

2.6.1. Other legislation relevant to these procedures and under which information may be shared includes:

- Academies Act 2010;
- the Children Act 2004;
- the Learning and Skills Act 2000 (S 117);
- the Data Protection Act 2018;
- the UK General Data Protection Regulation;
- Crime and Disorder Act 1998;
- Equality Act 2010;

- Education and Inspections Act 2006;
- Education Act 2011;
- Care Act 2014;
- Children and Families Act 2014.
- Any emergency public health legislation

2.6.2. These procedures reflect the requirements of the *Protocol on Data Sharing and rationalisation in the Schools Sector* (DfES, rev. 2005).

3. What data will be collected?

3.1. The full list of data covered by this agreement is shown in [Appendix A](#).

3.2. This list covers all the known data needed by this agreement at beginning of the academic year.

3.3. If there are additions to this data set, then Education Providers will be informed through the normal communications channels.

4. How will the data be used?

4.1. The data will be used to complete statutory and legal responsibilities of the LA as detailed in [Appendix B](#).

4.2. Information will also be used to inform provision of LA Services to individual children to ensure their well-being and safety. It will be used to help identify children missing from education and to target intervention and support through monitoring of key indicators such as attendance and exclusions.

4.3. There may be other opportunities that arise during the year that the LA will make Education Providers aware of, seeking permission where needed.

5. How will the data be transferred?

5.1. Both parties must make sure that data is transferred by appropriate Security measures. These measures must agree to comply with the Data Protection legislation regarding security and to ensure that adequate security arrangements are in place, to protect the integrity and confidentiality of the information held.

5.2. By electronic transfer

5.2.1. The B2B (base to base) is the secure transfer of child level data from the Education Provider's Management Information System to the LA's Capita ONE central database system. Data is transferred via a secure internet connection. Data transfer from the Education

Provider's MIS is via a daily scheduled routine for basic student data and a weekly scheduled routine for Attendance data. Schools will be informed about any changes to data collection due to public health emergency legislation.

5.2.2. Educational Provisions that do not use B2B must make sure that any transfer of data is secure and must follow the instructions in 5.3 below when making their daily, weekly, termly, annual returns of data

5.2.3. For schools not using B2B, the timescale requirements for sending data are:

- **Attendance and Student Data:** weekly
- **Census Data File:** upon receipt of secure email from LA, as soon as the return is finalized and uploaded to Collect

5.3. By using secure email

5.3.1. It is best practice for schools to set up dedicated email accounts for key responsibilities in the school such as headteacher, designated safeguarding lead, SENCO e.g.

senco@nameofschool.somerset.gov.uk , rather than accounts in an individual staff member's name. These email accounts are then associated with a post rather than an individual, which ensures continuity of communication when staff leave the school and reduces the risk of data breaches.

5.3.2. For schools, the most secure way of sending email is by replying to an email from a name@somerset.gov.uk request. Secure sending would have been used by the LA meaning that the reply will be secure. Therefore, if data needs to be sent to the LA the Educational Provision should reply to an email sent from an name@somerset.gov.uk account.

5.3.3. When sending sensitive data to unknown email accounts (or as a new email):

- use the s2s transfer instructions from the DfE part of the GOV.UK site: (<https://www.gov.uk/guidance/school-to-school-service-how-to-transfer-information>).
- OR put use a secure sending tool such as Office Message Encryption or similar encryption tool.

5.4. Sending information by post

- 5.4.1. Limited personal or sensitive data can be sent by post but significant material including Social Care/Health information must be sent using special delivery;
- 5.4.2. Large parcels of personal and sensitive information such as case files should be double wrapped and sent by tracked special delivery or by bonded courier;
- 5.4.3. Include a return address on the envelope;
- 5.4.4. Label the envelopes and packets 'For Addressee only'.

6. Will the data be shared with others?

- 6.1. Information held in the LA's Capita ONE system may also be shared with other Children's Trust partners, such as the NHS, School Nurses, Avon and Somerset Police Authority (ASPA) and both private sector and third sector providers. This will only be done where to do so is in compliance with statutory guidance and legislation regarding the duty to co-operate to improve well-being of children and the relevant data protection acts.
- 6.2. Information from Capita One will also feed into the Transform Data View dashboard (see Appendix C)
- 6.3. Educational Provisions should share data with NHS and its agencies e.g. School Nurses to enable eye checks, immunisations and other statutory duties or roles to take place. See section 1.3
- 6.4. Where it becomes necessary to share data with other agencies for public health purposes, the LA will ensure that supplementary agreements are in place to facilitate this data sharing.

7. What does the Education Provider agree to?

- 7.1. If using B2B, the Education Provider will send daily updates of children's personal data (including exclusions) and weekly updates of children's attendance data.
- 7.2. Where not using B2B the Education Provider agrees to provide changes to the data at the times agreed to in para 5.2.3. These changes should be provided to the LA at the same time as the Education Provider management information system is updated.
- 7.3. For schools not using B2B: in the event of technical failure of the school's own data transfer system the Education Provider will notify the LA via the SCC Service Desk and resolve the issue in a timely manner and will commit to maintaining to provide the data in other ways as discussed with the LA.

- 7.4. Work with the LA to resolve any data discrepancies e.g. pupils appearing at multiple Education Providers.
- 7.5. Provide any additional statutory information in respect of any safeguarding issues or concerns such as the intention to remove a child from the school roll.
- 7.6. Educational Provisions must provide a Privacy Notice to data subjects that details the data that is collected and who it is shared with.

7.7. Attainment Data

- 7.7.1. Securely transfer data to the LA before the end of the academic year for the various Key Stage assessments in electronic format.
- 7.7.2. Provide individual performance data (not already covered by other data collections) for vulnerable groups of pupils to the LA to fulfil statutory obligations for these pupils.
- 7.7.3. Provide other assessments (not already covered by the other data collections) to facilitate analyses requested of the LA by Education Provider and the Headteacher Association if the Education Provider agrees to these arrangements and partakes in these groups.

7.8. Meetings around a child

- 7.8.1. The Education Provider must ensure that all personal data relating to Health and Social Care is securely collected, processed, transferred, and stored in accordance with the Data Protection Act.
- 7.8.2. The transfer of personal data between the Education Provider and the LA will always be by secure methods as listed in para 5, when requested by the LA.
- 7.8.3. Once the intervention involving the young person is complete the Education Provider should observe the relevant retention schedules for the data.

7.9. Young Carers data

- 7.9.1. Under the Care Act 2014 and the Children and Families Act 2014, teachers and other professionals have a duty to identify Young Carers.
- 7.9.2. This information will be collected as part of the B2B process if the Education Provider uses this process.
- 7.9.3. For Educational Provisions who do not use B2B, the LA will put in place a process to make sure that the data is transferred securely in line with the instructions in Section 5.

8. What does the LA agree to do?

- 8.1. Make the data available to Children's Services professionals via the Capita ONE system to reduce the need for multiple and frequent data requests made to the Education Provider directly.
- 8.2. Use the data that is collected via Capita One to populate Transform Data View and use the data for the purposes stated in Appendix C
- 8.3. Notify the Education Provider if they become aware of any inaccuracies or possible discrepancies in the data they receive to ensure that data held by both parties is accurate and up to date.
- 8.4. Provide advice and guidance to support the data transfer process.

9. Support from the LA

9.1. Management Information Systems (MIS)

- 9.1.1. The SSE MIS Support Service are the main support agents for Education Providers in maintaining their MIS. Schools who subscribe to the SSE MIS Support Service will agree to allow access to help with any required maintenance of the system. In addition, there are occasions when personal data has to be extracted from the Education Provider servers.
- 9.1.2. The LA will only take copies of data with the full agreement of the Education Provider and will ensure that the personal data is stored on the secure network at County Hall or on encrypted portable devices.
- 9.1.3. On occasions, the data may be sent to ESS SIMS so that they can solve an issue. On these occasions the Education Provider will always be asked for permission. The security of system used by ESS to ensure that the requirements of the Data Protection Act are met can be found on a document titled 'Quick Reference Guide – Customer Instructions for uploading data' which can be obtained upon request to the SSE MIS Support Service.
- 9.1.4. Where data is collected for Educational Provisions with their agreement for support purposes, the data will only be used for the purpose it has been collected for and will be securely deleted shortly after the issue has been resolved.
- 9.1.5. In supporting Education Providers with B2B, the SSE MIS Support Service will remotely support them through the SSE MIS Support Service level agreement and its statement regarding access to servers.

9.2. Finance Information

- 9.2.1. There are elements of personal data associated with finance such as funding for Education Providers taking excluded pupils.
- 9.2.2. In every case where personal data is involved the communication of the data will be through secure methods.
- 9.2.3. The Education Provider will ensure that all financial data sent from the LA is stored in a secure area and in accordance with the Data Protection Act 2018 especially those relating to the necessary retention periods.

9.3. School Census

9.3.1. The LA agrees to:

- Core IT will send a secure email to schools requesting the data ensuring that the reply will be secure;
- The LA agrees to work with the Education Provider to define and make available data held on the Capita ONE System for benchmarking and School to School Support.

9.3.2. The LA will support the secure transfer process by giving the Education Provider advice on the collection, recording and submission of the data required by the DfE.

9.4. Attainment Data

9.4.1. The LA will support the secure transfer process by giving the Education Provider advice on the collection, recording and submission of the data required by the DfE.

10. Data security breaches and reporting procedures

- 10.1. Under the terms of data protection laws each Education Provider is a Data Controller, as is the LA.
- 10.2. This means that each individual body is responsible and liable to report all serious data security breaches to the ICO.
- 10.3. The Education Provider must maintain appropriate levels of cybersecurity and ensure that they have systems and policies in place to minimise the risk of data loss through mistake, mismanagement or technical security breach.
- 10.4. In the case of Education Providers, the priority for the reporting of security breaches will be the Governors, the Head and the Data Protection Officer for the school.

- 10.5. It is helpful to inform SCC Service Desk as they may be able to offer advice or warn other Education Providers if the breach could affect them e.g. spam, phishing, software virus, spree of thefts etc. The Educator Provider should also consider reporting suspicious emails to the National Cyber Security Centre's [Suspicious Email Reporting Service \(SERS\) report@phishing.gov.uk](mailto:report@phishing.gov.uk)
- 10.6. The ICO regards data security breaches as:
- 10.6.1. Exposure to identity theft through the release of non-public identifiers e.g. passport number or NHS number;
 - 10.6.2. Information about the private aspects of a person's life becoming known to others e.g. financial, domestic, health or care circumstances.
- 10.7. The ICO will also consider the risk sensitivity of the data to individuals, and number of individuals affected.
- 10.8. Data security breaches may include the loss of unencrypted laptops, memory sticks, mobile devices, DVDs, paper files or other documents.
- 10.9. In the event of a data loss each Data Controller and their Data Protection Officer must investigate and record the data loss and must consider:
- 10.9.1. Informing the other concerned parties of the loss;
 - 10.9.2. Informing the LA Information Governance Team or other LA Officer;
 - 10.9.3. Informing the data subject of the loss.

11. Appendix A - List of Data Items transferred between Education Providers and the LA (as of August 2020):

Data Item	Statutory/Legal Reason and Purpose
<u>Pupil</u> Address Date of Birth EAL Ethnic Source Ethnicity First Language Forename Former UPN FSM Eligible/Date Gender Guardians Medical Flag Middle Names Mode of Travel NCY Preferred Forename Preferred Surname Religion Service Family Surname Traveller Family UPN Young Carer Young Carer Notes Young Carer Start and End Dates Youth Support Services Agreement Indicator	<p>To support the LA Statutory Function in many areas. Examples below:</p> <p><u>Admissions and Entitlements</u> - DfE Statutory guidance on Home to School Transport and associated legislation; SCC Home to School Travel Policy including discretionary transport section and SEN transport entitlement; Section 19 Education Act 1996 as amended by section 3A of the Children, Schools and Families Act 2010; DfE Statutory guidance Exclusion from maintained schools, academies and pupil referral units in England and associated legislation; DfE Statutory guidance Alternative provision; DfE Statutory guidance on School Admissions Code 2021, School Admissions Appeal Code 2012 and associated legislation; Eligibility checking service for free school meals for all Somerset schools including Academies that purchase this service; Eligibility checking of funding for 2-year-old Entitlement and Early Years Pupil Premium.</p> <p><u>Education Safeguarding Service</u> - To ensure education providers prioritise safeguarding work and that an education voice is available in all such discussions; meeting the needs of Working Together 2015 and Keeping Children Safe in Education 2021, Children Act 2004, Section 13. (Sections 14 - 16 refer to the functions, procedure and funding of Local Safeguarding Children Boards). Secondary - Local Safeguarding Children Boards Regulations 2006, SI 2006/90. The Local Safeguarding Children Boards (Amendment) Regulations 2010 - SI 2010/622 (under Children and Young Persons Act 2009).</p> <p><u>Traveller Education Liaison Officers</u> - Statutory duty to promote the educational achievement of vulnerable and disadvantaged groups; Statutory duty under the Equality Act 2010 for LA, schools and academies to have due regard for the need to eliminate harassment and discrimination, advance equality of opportunity, foster good relations and tackle prejudice; local authorities, schools and academies' statutory duty to set specific and measurable equality objectives and publish information.</p>
<u>School History</u> Boarder End Date Enrolment Status LA Number Part Time Registration Group School Name School Number Start Date	<p>The Education Act 1996; Children's Act 2004 – allows Education Providers to inform the LA of Attendance in a timely manner. Safeguarding purposes.</p>
<u>Attendance</u> Attendance Mark Absence Reason	<p>The SEND Code of Practice provides Statutory guidance on duties, policies and procedures relating to Part 3 of the Children and Families Act 2014 and associated regulations. It relates to children and young people with Special Educational Needs (SEN).</p>
<u>SEN</u> NHS Number (Proposed) SEN History SEN Need SEN Status/Date	<p>School Standards and Framework Act 1998; Education Act 2002; Education and Inspections Act 2006; DfE Guidance 2012 – allows Education Providers to inform the LA of Exclusions in a timely manner. Safeguarding purposes.</p>
<u>Exclusions</u> Category End Date Reason Start Date	<p>School Standards and Framework Act 1998; Education Act 2002; Education and Inspections Act 2006; DfE Guidance 2012 – allows Education Providers to inform the LA of Exclusions in a timely manner. Safeguarding purposes.</p>

12. Appendix B

	Data Description	Purpose	From	To	Statutory/Support	Timescales	Mechanism
Processes							
1	Student Core Data (as per above)	Supports Statutory Duties	Education Providers	Local Authority	Supports LA Statutory Function	Daily/Weekly/Termly/Annually	B2B from MIS, or alternative School data transfer system
2	School Census	Statutory Requirement from DfE for LA Education Providers	Education Providers	Local Authority	Statutory/Supports LA Statutory Function	Termly	Secure email from Core Data Team to school and reply from school
3	Early Years Foundation Stage (EYFS)	Statutory Requirement from DfE	Education Providers	Local Authority	Statutory	Annually	MIS (file export or B2B) or alternative School data transfer system
4	Phonics Screening Check	Statutory Requirement from DfE	Education Providers	Local Authority	Statutory	Annually	MIS (file export or B2B) or alternative School data transfer system
5	Key Stage 1 (KS1)	Statutory Requirement from DfE	Education Providers	Local Authority	Statutory	Annually	MIS (file export or B2B) or alternative School data transfer system
6	Key Stage 2 (KS2)	Supports Reporting to LA and Education Providers	DfE	Local Authority	Supports LA Statutory Function	Annually	File download from DfE
7	Key Stage 4 (KS4)	Supports Reporting to LA and Education Providers	DfE	Local Authority	Supports LA Statutory Function	Annually	File download from DfE
8	GCSE Results Day	Supports Reporting to LA and Education Providers	Education Providers	Local Authority	Supports LA Statutory Function	Annually	MIS (file export or B2B) or alternative School data transfer system
9	A Level Results Day	Supports Reporting to LA and Education Providers	Education Providers	Local Authority	Supports LA Statutory Function	Annually	MIS (file export or B2B) or alternative School data transfer system

Information Sharing Arrangement Transform Data View for Educational Settings

Parties

Somerset County Council

Education Settings; of:

The types of roles in these settings are:

- Designated Safeguarding Leads
- Team Around School Co-ordinators
- Parent and Family Support Advisers
- SENCOS

About this document

This document acts as a Tier 2 Information Sharing Agreement (ISA) between the above parties and Somerset County Council and must be read in conjunction with the Data Sharing agreement between Somerset County Council and Settings, Academies, and other Education Providers.

Version Control

Author/Owner	Lucy Wilkins / Gill Bawler, SCC
Consulted	Amy Brittan Schools DPO
Date First Published	01/09/2022
Date Last Reviewed	N/a
Date of Next Review	31/08/2022

	Version	Date	Change	Author
1	0.1	10/03/2021	First draft	Lucy Wilkins
2	0.2	31/08/2021	Second draft following consultation with SSE DPO	Amy Brittan
3	1.0	01/09/2021	Final Version	Lucy Wilkins

1. Introduction

1.1. Building on the success of information sharing under the Supporting Families (Troubled Families) programme, SCC have developed a secure application to allow core professionals access to key information about families in order to identify families of multiple disadvantage, provide early intervention support and improve the welfare of families.

1.1. It is therefore necessary to share information between partners to:

- 1.1.1. bring together data to understand needs at an individual, family and population level
 - 1.1.2. improve or target appropriate and timely support to individuals or households, to prevent the escalation of issues.
 - 1.1.3. improve the physical, mental, emotional, social or economic well-being of individuals and families.
- 1.2. To ensure all professionals working with the family can understand the circumstances of the family, and tailor their support effectively, information will be made available through a front-end viewer called Transform Data View.
- 1.3. “The transform data view provides early intervention opportunities and presents multi-agency data pertaining to social issues to a range of frontline professionals. The integration of this new data will elicit a deeper and broader understanding of the multiple issues affecting individuals/families. It will reduce duplication and resource for practitioners supporting the family, as it contains headline detail on assessments and current and historic involvement, not just with statutory services, but commissioned providers, such as the drug and alcohol service and the voluntary and community sector.”¹
- 1.4. Ultimately this results in the improvement of the physical, mental, emotional, social or economic well-being of individuals or households.
- 1.5. This Information Sharing Arrangement (ISA) details the sharing of personal data between agreed parties to meet the purpose of improving access to information in a timely manner. This will enable education professionals to have a better understanding of a family’s complexities and improve joined up working
- 1.6. It aims to set out and record parties’ mutual understanding of what data will be shared, the reason for doing so and how it will be treated. The intention of this agreement is to ensure consideration of and compliance with the relevant provisions of the Digital Economy Act 2017 and Data Protection Legislation by all parties.
- 1.7. On signing this agreement all signatories accept and adopt the practices within, in addition to those defined in the Data Sharing agreement between Somerset County Council and Settings, Academies, and other Education Providers.

2. Background

- 2.1. One of the Supporting Families Programme’s (previously named Troubled Families Programme) key analytical assets is Transform. Transform is a data warehouse, which draws together information

¹ SCC Transform Business Case

from over 35 data sets, matching individual household members and their vulnerabilities to an address, which enables the practitioner to understand the family's circumstances holistically. It has made possible, for the first time, a joined up collaborative view on vulnerability and a true picture of threat, harm and risk within a household. Transform provides early intervention opportunities and presents multi-agency data pertaining to social issues, currently available to professionals internal to SCC. The integration of this data gives a deeper and broader understanding of the multiple issues affecting individuals/families, along with involvements, assessments and education attendance data.

- 2.2. Somerset has a range of Specialist and Early Help Practitioners, Designated Safeguarding Leads and Multi-Agency forum coordinators, external to SCC who are identifying support or supporting families. These practitioners currently have no sight of the vulnerabilities and risks associated with the family, historic assessments, or involvements with Children's Services or the wider early help system
- 2.3. Evidence from a number of Serious Case Reviews (SCR) has highlighted the lack of joined up IT systems as a failing. Further findings from SCR's are that holistic assessments are not routinely made and that some agencies respond reactively to each situation rather than seeing the whole context.

3. Business case, and purposes of onward sharing via Transform

- 3.1. To enhance the way organisations work together to share information that is necessary and proportionate to effectively support individuals and their families
- 3.2. To enable professionals to have a holistic view of known vulnerabilities and complexities of the individual and the family they are supporting
- 3.3. To enable professionals to tailor their support accordingly using the holistic oversight
- 3.4. To reduce duplication of professional involvement and assessments
- 3.5. To enable SCC to provide information to partners for the purpose of ensuring we meet our obligations as a public authority
- 3.6. In addition to the purposes listed here, onward sharing will allow key professionals
 - 3.6.1. working with the family to understand the involvement of other key organisations, with the ability to contact the Lead Professional more efficiently.

- 3.6.2. Enable key professionals to identify in a timely manner other support agencies reducing the administrative burden on professionals and reducing the risk of inaccurate and out of date information being used.
- 3.6.3. to understand assessments that have taken place with the family, identifying the contact details of the author.
- 3.6.4. to tailor appropriate support with an increased holistic view, to support the prevention of escalation of issues.

4. Benefits of the intended sharing:

- 4.1. To support and facilitate early intervention.
- 4.2. To ensure all signatories to this agreement have the ability, confidence and trust to share information, so that those who are subject to, or likely to be subject to, harm, neglect or disadvantage can be identified in a timely manner, which will help to protect and meet the needs of vulnerable people.
- 4.3. To enable better coordinated activities between agencies, reducing duplication and a more integrated approach.
- 4.4. To enable an enhanced level of identifying risks
- 4.5. For the full business case details please see appendix 1

5. Public Service Delivery Power Objectives (PSD)

- 5.1. The above business case and benefits enables the three objectives of the PSD power to be met.
- 5.2. It allows condition one to be met as the lead professional purpose is to ensure that they improve the service they provide to individuals or households thus helping them to minimise the escalation of issues
- 5.3. It allows condition two to be met as tailored support will contribute to the improvement of the well-being of individuals or households
- 5.4. It allows condition three to be met as the local authority has a duty to provide services, and good information sharing will support the local authority to improve the services being provided to children, and their families
- 5.5. All partners with whom the information is shared will only use that information for the purposes listed above unless they are satisfied that use of that data meets one or more of the criteria given under section 40 of the Digital Economy Act.²

² <https://www.legislation.gov.uk/ukpga/2017/30/section/40/enacted>

6. Consequences of not sharing information

- 6.1. increased risk that people do not receive the support or the services they require in a timely manner.
- 6.2. risk that burdens will be placed on people to repeatedly supply information to access the services they require.
- 6.3. Increased resource impact for lead professionals to identify and contact other professionals who have previously worked with the family
- 6.4. Lead professionals will not be aware of the full picture of the family's issues, and therefore plans may not include all of the complexities that the family are experiencing
- 6.5. professionals will be required to check multiple systems to have a holistic view
- 6.6. The professional may not have access to the relevant systems to provide a holistic view.

7. Information to be shared

- 7.1. The Transform Data View will provide a snapshot of the vulnerability flags, risks, assessments, involvements and attendance data, including contact details of key professionals.
- 7.2. Information will only be shown where there has been a historic involvement within the last two years.
- 7.3. Fields will indicate either
 - 7.3.1. no information on database
 - 7.3.2. historic
 - 7.3.3. current
- 7.4. The display will consist of the following fields:
- 7.5. **Personal details**
 - 7.5.1. Name
 - 7.5.2. Address
 - 7.5.3. DOB
 - 7.5.4. Student ID
 - 7.5.5. NHS ID
 - 7.5.6. LCS Case ID
- 7.6. **Vulnerability Criteria (flags showing areas of vulnerability)**
 - 7.6.1. Active Social Care / Early help involvement
 - 7.6.2. Known to Social Care / early help
 - 7.6.3. Known to other supporting services
- 7.7. **Individual flags (flags showing CSC involvement)**
 - 7.7.1. Child Looked After
 - 7.7.2. Child Protection

- 7.7.3. Child in Need
 - 7.7.4. Young Carer
 - 7.7.5. Education & Health Care Plan
 - 7.7.6. Special Educational Needs / Children with Disability support
 - 7.7.7. Safeguarding Notifications
- 7.8. **Transform Vulnerability (flags showing Transform criteria met)**
- 7.8.1. Education
 - 7.8.2. Health
 - 7.8.3. Worklessness
 - 7.8.4. Need Support
 - 7.8.5. Services supported
 - 7.8.6. Substance misuse
 - 7.8.7. Crime
 - 7.8.8. Anti-Social Behaviour
 - 7.8.9. Domestic Violence
- 7.9. **Involvements (list of agency involvements i.e. CSC, FIS)**
- 7.9.1. Agency
 - 7.9.2. Start and End Date
 - 7.9.3. Worker
 - 7.9.4. Lead Professional Email Address
- 7.10. **Assessments (Assessment forms i.e. Child in need plan)**
- 7.10.1. Assessment type
 - 7.10.2. Assessment date
 - 7.10.3. Document creator
 - 7.10.4. Assessment creator email address
- 7.11. **Education (School term attendance)**
- 7.11.1. Term start
 - 7.11.2. Term End
 - 7.11.3. School Name
 - 7.11.4. Attendance percentage
- 7.12. Any information shared under this Agreement must only be used for the Purposes outlined in section 3 above.
- 7.13. There may be, on a case by case basis, further information disclosed to the professional by an appropriate SCC officer. This will be proportionate and necessary to the enquiry and will be covered under the relevant information sharing protocols already in place and the education settings own safeguarding policies.
- 7.14. If a lead professional requires clarification on the data displayed they should email transform@somerset.gov.uk
- 7.15. The onward sharing of this information is not permitted under this information sharing arrangement, unless there is a safeguarding concern where current protocols should be followed.

7.16. For data flow map please see appendix 2

8. Legal gateways, and relevant legislation

- 8.1. Each party must be satisfied that they have checked and verified their own legal gateways for processing the information being shared.
- 8.2. Digital Economy Act 2017, Part 5, Section 35
 - 8.2.1. This allows the disclosure of information to improve public service delivery.
 - 8.2.2. A person (as specified in Schedule 4 of the Act) may disclose information held by them in connection with any of the person's functions to another specified person for the purposes of an objective which is a specified objective in relation to each of those persons.
 - 8.2.3. The specified objective is the multiple disadvantage objective outlined in paragraph 2.1 to 2.6 of the schedule of The Digital Government (Disclosure of Information) Regulations 2018.³
- 8.3. UK GDPR Article 6.1.e – Necessary for the performance of a task carried out in the public interest or in the exercise of official authority
 - 8.3.1. The data sharing is necessary as it provides a holistic view of the complex issues that a family faces and allows professionals working with the family to plan support appropriately
 - 8.3.2. The data sharing is proportionate as it is limited to the categories described in Appendix 4, and the organisational and technical measures described in section 12.
- 8.4. UK GDPR Article 9.2.b and 9.2.h – Social Security and provision of social care
 - 8.4.1. The data sharing is necessary in supporting the Local authority and its partners functions in reducing the impact of multiple partners involved in service provision having limited or different information
 - 8.4.2. The data sharing is proportionate as it is limited to the data sharing described in 6.2.2.
- 8.5. DPA Schedule 1 - Social Protection and social care provision
 - 8.5.1. Condition 1 of this schedule provides conditions to share information for the purpose of Social protection
 - 8.5.2. Condition 2 of this schedule provides conditions to share information for the purpose of providing Social Care and managing Social Care systems and services

³<https://www.legislation.gov.uk/uksi/2018/912/schedule/made>

- 8.5.3. The data sharing is necessary to support the Local authority and its partners in reducing the impact of Social Protection Risks on children and families
- 8.5.4. It is necessary to ensure that the local authority is able to provide Social care in an effective way, and reduce the impact and burden on families and children by having to repeatedly share information

9. Appropriate Policy Document (APD)

- 9.1. In order to process Special Category and Criminal conviction data each organisation is required to have in place an Appropriate Policy Document (APD) which meets the requires set out in Schedule 4 of the Data Protection Act.
- 9.2. SCC's APD is available upon request to informationgovernance@somerset.gov.uk
- 9.3. Schools will ensure that they have an appropriate policy document in place that meets the requirements of Schedule 4 of the data protection legislation.

10. Access to data protocol

- 10.1. Access to the data will be through the read-only Transform Data View
- 10.2. Each organisation will ensure that they have carried out their own checks with regards to the legal basis of processing the data under the Digital Economy Act and Data protection legislation before signing this agreement
- 10.3. A secure link will be issued once
 - 10.3.1. training has been completed
 - 10.3.2. DBS checks and safer recruitment checks have been verified
 - 10.3.3. The partner organisation signs up to this ISA

11. Accuracy and adequacy of data

- 11.1. Systems are in place to ensure that the data being matched in the Transform Data Warehouse is adequate and accurate.
- 11.2. However should a lead professional identify an inaccuracy they must inform the Transform team of that error and the Transform team will take steps to inform the originating organisation of the inaccuracy. Contact transform@somerset.gov.uk

12. Retention of data

- 12.1. The data will be provided in read-only format, and screen shots or notes taken of the data will not be permitted unless it is specific to the professional's purpose or where there is a safeguarding concern and this is in line with the education setting safeguarding and data protection policies
- 12.2. The data available under the DEA provided in Transform data view will be restricted to two years historic data, unless an incident, flag, assessment or involvement has been identified in the last two years. Where this is the case a chronology of historic involvements (intervention from Children Social Care / Early Help) would be visible.

13. Supporting rights of data subjects:

13.1. Data subjects have the right to be informed about how their personal data is being processed. Who it is being shared with, and the right to object in certain circumstances to the processing of that data. (see appendix 3)

13.2. All parties will ensure that they understand what rights data subjects have and how to process these.

13.3. Right to be informed:

13.3.1. All parties will ensure that individuals are notified of the data sharing and use of the data via their organisations privacy notices made available to individuals when they become known to the organisation.

13.3.2. All parties will ensure that they update their privacy notices to reflect the data sharing under this agreement and where applicable inform the data subject.

13.3.3. SCC will also ensure the use of Transform Data View is specified on their privacy notice webpage:
www.somerset.gov.uk/privacy

13.4. Right of access to data:

13.4.1. The Transform data view is read only and will show a snapshot of involvements, assessments, flags, identification details and education data.

13.4.2. If a data subject puts in a request specifically for the information viewed on Transform Data View, they should be directed to Somerset County Council, who subject to the Data Protection Act legal requirements and any exemptions that may apply, will provide a copy of the information held at that point in time, with an audit as to who has accessed the data and when.

If there was a safeguarding need for the education setting to copy or record the information from Transform Data View, at the time of access the education setting will become the data controller and will be subject to their own DSAR process.

13.5. Request rectification or correction of data, or a request that their data is erased or deleted (The right to be forgotten)

13.5.1. As the data on Transform data view has been pulled from multiple datasets a request for rectification or correction of data will be dealt with by the originating organisation.

13.5.2. The request for erasure is unlikely to apply as the data is being processed under legislation, however an individual still has the right for this to be considered.

13.5.3. If a data subject puts in a request specifically for the correction, rectification or erasure of data viewed on Transform Data View, they should be directed to Somerset County Council, who subject to the Data Protection Act legal requirements and any exemptions that may apply, will process their request and aim to provide a response within one month.

13.6. Request the restriction of processing if in dispute

13.6.1. As the data on Transform data view has been pulled from multiple datasets a request for restriction must be directed at all organisations using the data.

13.6.2. If a data subject puts in a request specifically for the restriction of data viewed on Transform Data View, they should be directed to Somerset County Council, who subject to the Data Protection Act legal requirements and any exemptions that may apply, will where applicable restrict the data whilst they consider the objection / rectification of data, and inform all relevant partner organisations.

13.7. Object to a request that we stop processing your data

13.7.1. A request objecting to the use of the data may be directed at any organisation using it.

13.7.2. If a data subject puts in a request specifically for the objection of data viewed on Transform Data View, they should be directed to Somerset County Council, who subject to the Data Protection Act legal requirements and any exemptions that may apply, will where applicable consider the objection, and where necessary take the relevant action required. They will inform all relevant partner organisations and the data subject of the outcome.

13.8. Right to complaint to the ICO

13.8.1. Data Subjects have the right to be informed of how to complain to the ICO.

13.8.2. Where parties are notified of a complaint being submitted to the ICO, the party will inform Somerset County Council who will liaise with the party to ensure that the complaint is dealt with swiftly.

13.9. All parties should inform the data subject that their request needs to be directed to Somerset County Council, and that with the data subject's permission they will forward that request to SCC at transform@somerset.gov.uk

14. Security measures relevant to the Transform Data View:

14.1. Organisational measures

- 14.1.1. All users requesting access will be granted permission based on their business need to view the information
- 14.1.2. Users will sign up to a Data Protection statement which outlines their responsibilities to ensure data is secure
- 14.1.3. Users with access will have a current basic DBS clearance, and will be in a role where they handle sensitive information around safeguarding
- 14.1.4. Access will only be provided once a professional's email address has been verified by SCC IT and the user
- 14.1.5. Access will only be provided once the employer has confirmed that the professional was appointed under a Safer Recruitment process.
- 14.1.6. Access to Transform Data View will only be provided once the professional's organisation has signed up to their relevant Information Sharing Agreement having due regard to the aforementioned code of practice.

14.2. Technical measures

- 14.2.1. Data is held securely on SCC systems hosted within the Council's secure network.
- 14.2.2. The system does not permit save, download or print functions. Access and viewing of data is fully audited.
- 14.2.3. Data regarding the category 'Transform Vulnerability' will be restricted to two years. Involvements will show as historic if a criteria has been met that is more recent
- 14.2.4. Data is minimised so the only information available via specific vulnerability flags are categorised as "no information on database", "historic" or "current" and whether any assessments have taken place and the professional that has done the assessment
- 14.2.5. Automated Fuzzy matching processes, automated address cleaning scripts and automated data cleansing forms will ensure accuracy of data.
- 14.2.6. Users will report back to Transform data warehouse team any inaccuracies they identify via an MS form, and the Transform Data team will inform the relevant asset owner.

14.2.7. The system has audit functionality, which captures user access, time and date stamp and the data subject they have accessed.

14.2.8. Somerset County Council has conducted a Data Protection Impact Assessment on the Transform Data View and this is available upon request to informationgovernance@somerset.gov.uk

15. Code of Practice Security Requirements (1.4.49)

15.1. The code of practice requires

15.1.1. public authorities and receiving parties should factor the standards and protocols that apply to their organisation when providing or receiving information before agreeing appropriate standards and protocols. All parties should be satisfied that they provide a level of security that is both appropriate and meets or exceeds their own standards and protocols.

15.1.2. each party involved in the data share must make sure effective measures are in place to manage potential or actual incidents relating to the potential loss of information; and

15.1.3. public authorities and data processors, together with any other additional third parties, must be fully engaged in the resolution of a potential or actual data incident. The responsibilities of each party in the event of a potential or actual loss of information must be clearly defined in the information sharing agreement or security plan. The controller has a responsibility to inform the ICO of a breach where the relevant thresholds are met

16. Data breaches:

16.1. If any potential or actual data incidents occur as a result of the use of Transform Data View, they will be managed by Somerset County Council with the full support of the party involved in the breach

16.2. The parties will notify Somerset County Council as soon as they are made aware, and without delay of a breach.

16.3. Contact should be made with SCC Information Governance team on informationgovernance@somerset.gov.uk

Review date: TBC

This agreement will be reviewed annually in line with the Overarching Data Sharing Agreement 'Somerset Local Authority / Schools Data Sharing Agreement, to establish if the sharing remains necessary, still operates as intended and, has or is, achieving the intended benefits. In the event that this Tier 2 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 agreement within their respective organisations, to interested parties and the wider public as necessary.

Signatories:

By signing this document, I accept that the organisation which I represent will be bound by any conditions imposed in both this document and in the overarching Information Sharing Protocol, which this organisation has previously signed.

Party 1 - Organisation name: Somerset County Council

Name: Julian Wooster
Role: Director of Children's Services
Date:

Signed

Party 2 - School name:

Name:
Role:
Date:
Signed

Transform: *The updated version of the Supporting Families database draws together information from a wide range of data sources and presents a single view of the individuals' vulnerabilities, interactions and assessments.*

Summary

This report addresses proposals as to how the Transform database can be made accessible to wider partners through Transform Data View (front end viewer).

Background

One of the Supporting Families programmes key analytical assets is Transform. This data warehouse draws together information from a number of data sets, matching individual vulnerabilities to enable the practitioner to understand the family's circumstances. It has enabled for the first time a joined up collaborative view on vulnerability and a true picture of threat, harm and risk within households. It provides early intervention opportunities and presents multi-agency data pertaining to social issues to a range of frontline professionals. The integration of this new data will elicit a deeper and broader understanding of the multiple issues affecting individuals/families. It will reduce duplication and resource for practitioners supporting the family, as it contains headline detail on assessments and current and historic involvement, not just with statutory services, but commissioned providers, such as the drug and alcohol service and the voluntary and community sector.

The additional benefit from Transform is that data captured supports a more strategic understanding of the county and the issues, risks and vulnerabilities experienced by Somerset's families. It is also capable of informing service planning and the more efficient allocation of resources and to provide intelligence for targeted focused interventions. Transform enables more effective and simplified information sharing, whilst also providing the data to drive improved analysis.

Aims and objectives

Transform has three primary aims:

1. To bring together data to understand needs at an individual and family level
2. the improvement or targeting of appropriate support to individuals or households to prevent the escalation of issues.
3. The improvement of the physical, mental, emotional, social or economic well-being of individuals and families.

Consultation

A range of key stakeholders, including the Voluntary Community Sector, Lead Professionals and agencies have been consulted through face to face engagement, workshops, presentations and virtual sessions. Use case task and finish groups have provided insight and helped shape the 'version one' Family Data View. During this consultation the need from partners was evident, with the greatest need being from schools.

Current Usage

Transform is currently used internally at Somerset County Council; this includes health visitors and school nurses, Children's Social Care, First Response, the Early Help Hub, the Family Intervention Service and the Education Safeguarding Service. The outcome of the consultation has evidenced the need for access to wider practitioners such as Designated Safeguarding Leads in schools and District Councils, Parent and Family Support Advisers, SENCO's, Heads, Team Around the School and One Team Coordinators.

Information Governance and security

The information is shared under part 5 of the Digital Economy Act (DEA) 2017, Public Service Delivery Power¹. The requirements of this power have been met and are published on the Gov.UK register². Where the partner is not named as a trusted partner in the DEA, an alternative legal gateway has been specified and named.

The security of the information has been paramount in the developing of the software. Users are required to have certified basic DBS clearance and evidence is required before permissions are granted. Access is through a weblink, using existing professional It log in to gain access.

The system is 'time stamp' auditable. Any data breeches will be reported initially to Somerset County Council (SCC) and then investigated jointly between the partner and SCC. The Information Sharing Agreements for each data source and user details the usage agreement for each partner and the confidentiality of the information.

Benefits

The long-term benefits have been identified and Transform, as a project is included in the Digital Customer strand of the ICT Digital Transformation Programme, which will track Transform activity, with strategic buy in at the highest level.

¹[Code of Practice for public authorities disclosing information under Chapters 1, 3 and 4 \(Public Service Delivery, Debt and Fraud\) of Part 5 of the Digital Economy Act 2017 - GOV.UK \(www.gov.uk\)](#)

²[Digital Economy Act information sharing powers and objectives register \(culture.gov.uk\)](#)

Transform is pivotal to the changes in multi-agency working. The approach to identifying multiple vulnerabilities in a household has already proven successful in transforming the lives of over 3000 families in Somerset. It allows services to quickly identify those families most in need and target resources appropriately.

The information generated can provide the identification of 'hot spots' of need and enable a more strategic approach to service provision. This is particularly valuable with the current limitations on public sector funding.

It identifies multiple agencies working with a family to enable a joined-up approach and reduce duplication, a benefit to families and the public purse.

How the data will be shared

Transform Data View is accessed through a secure link. Access will be granted following training (delivered by SCC), confirmation of a certified basic DBS clearance and confirmation that the Safer Recruitment process was adhered to on appointment.

Retention of data

All parties will abide by their generic retention schedules, and not hold data for any longer than is required for the purpose it was collected.

The data will be provided in read-only format, and screen shots or notes taken of the data will not be permitted unless it is specific to the professional's purpose or where there is a safeguarding concern.

The data available under the DEA provided in Transform data view will be restricted to two years historic data, unless an incident, flag, assessment or an involvement has been identified in the last two years. Where this is the case a chronology of historic involvements (intervention from Children Social Care / Early Help) would be visible.

Security measures

Organisational

- All users requesting access will be granted permission based on their business need to view the information
- Users will sign up to a Data Protection statement which outlines their responsibilities to ensure data is secure.
- Users with access will have a current basic DBS clearance, and will be in a role where they handle sensitive information around safeguarding
- Access will only be provided once the employer has confirmed that the professional was appointed under a Safer Recruitment process.
- Access to Transform Data View will only be provided once the professional's organisation has signed up to their relevant Information Sharing Agreement having due regard to the aforementioned code of practice.

Technical

- Data is held securely on SCC systems hosted within the Council's secure network.

- The system does not permit save, download or print functions. The system has audit functionality, which captures user access, time and date stamp and the data subject they have accessed.
- Data is minimised so only information available via specific vulnerability flags are categorised as 'no information on database', 'historic' or 'current' and whether any assessments have taken place and the professional that has done the assessment.
- Automated Fuzzy matching processes, automated address cleaning scripts and automated data cleansing forms will ensure accuracy of data.
- Users will report back to Transform data team any inaccuracies they identify via an MS form, and the Transform Data Warehouse team will inform the relevant asset owner.

SCC has conducted a Data Privacy Impact Assessment on Transform Data View and this is available at www.somerset.gov.uk/privacy

Timeline

Phase one (April 2021) will include external practitioners from:

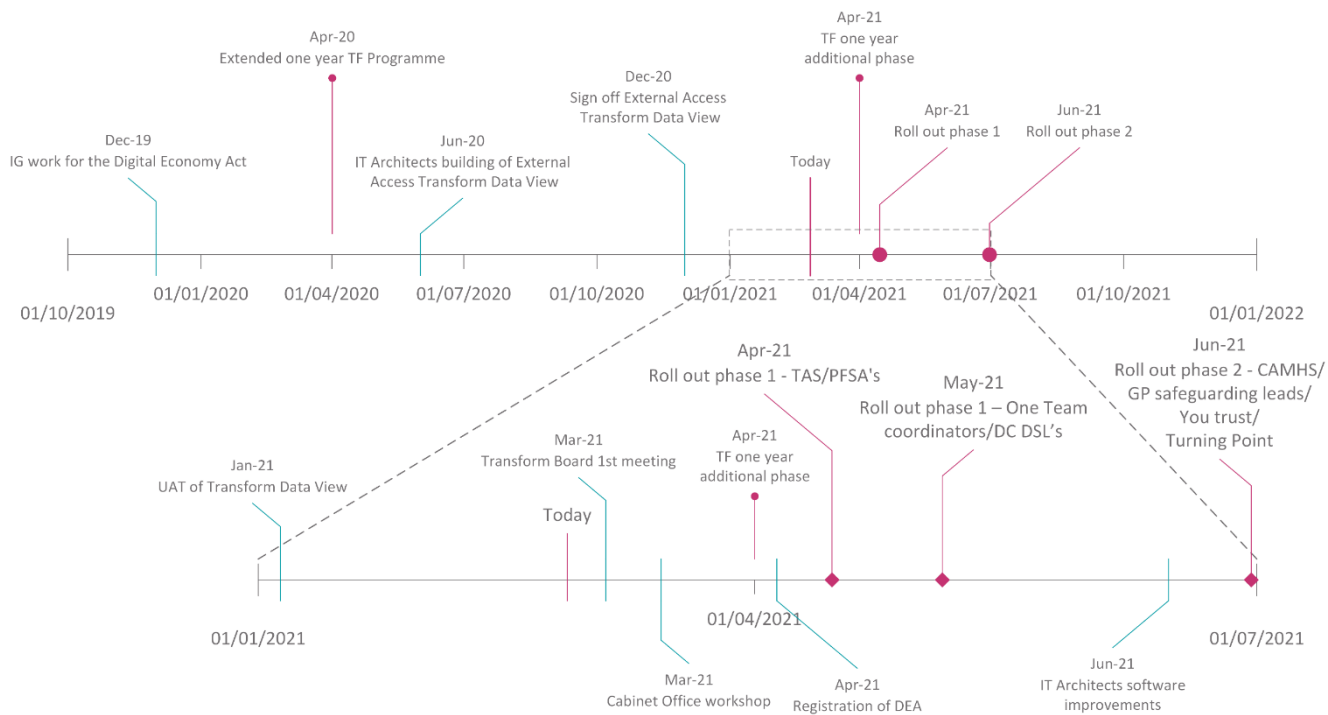
- Education – Team Around the School Coordinators, Parent and Family Support Advisors, Special Educational Needs Officers (SENCO's) & Designated Safeguarding Leads
- District Councils – Designated Safeguarding Leads & One Team Coordinators

Phase two (summer 2021) will include external practitioners from:

- Health – GP Safeguarding leads and lead Business Support from each practice, CAMHS practitioners

Phase three (Autumn 2021) will include external practitioners from You Trust, Domestic Abuse Service and Turning Point, Substance Misuse workers

Appendix One – Transform Data View timeline



Appendix 2 – Data Flow Map

