ADVICE ON USING THE DATA MAPPING TOOL

The most important task that you need to do before GDPR comes into force on 25th May 2018 is to map the personal information that you hold and share as a school, academy or MAT and the simple tool available with this update is designed to help you do this.

We are aware that some of you have already made use of mapping tools provided by other organisations, so you do not have to complete this tool if you have already captured all the information using a different tool.

There is guidance below for completing each section of the tool. The first 6 columns deal with the information *you hold and make use of internally* within your organisation, in order to educate and support children and in relation to staff.

The last 4 columns deal with the information *you share externally with other organisations*, usually for statutory or contractual purposes.

You should list each type of personal data separately, and then for each of those, explain how you obtain that information, your justification for holding it, where is it held, and what risks exist in relation to you holding and using the information.

In addition, for any information that you share with others, or hold on external servers, you also need to set out the legal justification for sharing personal information with that service or agency and where it held, Taking each of the tool's columns in turn:

Data Held (Column B)

You need to ensure that you list all the personal data that you hold about pupils, staff, parents and others. Personal data is defined as any information which relates to an identified or identifiable person, and which either identifies that person or, in conjunction with other information held, allows a person to be identified or categorised in some way. This will therefore include all of the following information, plus much more:

- Name
- Address and Contact Details
- Job Details
- Date of Birth
- Educational Record, including Special Educational Needs
- Medical Information
- Safeguarding Information
- National Insurance Number
- Gender Identity
- Ethnicity

You should complete this both for information that you hold internally, and that which you share, or send to, others.

Data Source (Column C)

You need to keep a record of where each type of information comes to you from. It is likely that data of a similar type will be received from similar sources, so for example names of children to attend the school will come initially either from a local authority's admissions service or be provided directly by parents. Contact details for family members will usually come via a data collection form completed by parents. SEN information may come from

other schools or from internal or external assessments. If there are multiple sources then list all the likely ones in this column.

Legal Reason for Processing (Column D)

GDPR requires a legal justification for the holding and sharing of all personal information. Therefore for each type of personal data you hold, and for each agency / service you share it with, you need to be able to explain why the law allows you to do so. Please be aware that the law in this area is changing slightly under GDPR and as such you need to be able to prove one of the following in relation to standard personal information such as names, addresses and dates of birth:

- Consent has been given;
- Necessary for the performance of a contract to which the data subject is a party;
- Necessary to comply with a statutory or other legal obligation;
- Necessary to protect the vital interests of the data subject or another person;
- Necessary in the public interest

Please note that the justification of holding and processing information for the purposes of 'legitimate interests pursued by the controller' is no longer available to a public body such as a school or academy (the new GDPR does not allow this), which means that - unless consent has been given, a child is at risk, or a legal obligation applies - it is very difficult to justify the holding or sharing of personal information about a person.

For 'special' categories of personal information, the rules are even tighter. 'Special' personal data includes any information which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, 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. This might therefore include some staffing information, and also information of a sensitive and personal nature about pupils, such as some special educational needs and medical information. In these circumstances you need to be able to explain why the law allows you to hold/share the information (i.e. which one of the five legal reasons above applies) and also prove one of the following reasons applies:

- Consent has been given;
- Necessary in relation to specific employment and social security legislation;
- Necessary to protect the vital interest of the data subject or another person where the person is incapable of giving consent;
- Personal information has been made public by the data subject
- Necessary in relation to legal proceedings;
- Necessary for reasons of substantial public interest;
- Necessary for medical or social care or public health reasons.

Where is the Data Stored? (Column E)

It is vital that you keep personal information secure, whether it is held in paper form or electronically. Therefore please set out in this section how information is held internally in the first section, and how it is transferred to and then held by external agencies, to the best of your knowledge, in the second section. This should be straightforward for information held internally but may require research for external systems, in particular where they are web-based. Where is the server located for these services? Is it in the UK, elsewhere in the EEA, in the United States, or even somewhere else in the world? This will have particular

implications as data security law is different in different parts of the world, but you need to be assured that standards applicable in the UK apply.

Risks (Column F)

It is important that you give thought to risks associated with the holding, using, transferring and sharing of personal information. Could it get into the wrong hands or be used for the wrong purposes? What safeguards have you put in place? Your DPO can support you in the process of understanding risk.

Who has access to the Data? (Column G)

You need to identify which individuals or categories of staff within your organisation have access to the data

Data Sharing (Columns H-K)

These parts of the tool only need to be completed if you share the data with external bodies.

If you answer yes in Column G, you then need to list each of the external agencies and organisations that you share information with. This will include public sector bodies including local authorities, central government (particularly for academies) and the NHS, but also external contractors who provide educational services both in person (such as specialist teachers) and online (such as Class Dojo). All web-based systems will need to be included if they hold any pupil, parent or staff information inputted by the school, but do not need to be included if the school never input any personal information into the system themselves (including names of pupils or staff).