RESPONSE FROM SHEFFIELD CITY COUNCIL

Art No	Title & Description	Comments/views
1. Supervisory Authority		
Article 51 Recital(s) 117,118, 119	**Supervisory Authority** The 1998 Data Protection Act applies throughout the UK and the Information Commissioner has sole responsibility for ensuring compliance.	Article 51(1) of the GDPR provides discretion for Member States to have one or more independent public authorities with responsibility for monitoring the application of the GDPR which may be attractive to devolved parliaments/assemblies in Wales, Scotland and Northern Ireland.
Article 53 Recital(s) 121	**General conditions for the members of the supervisory authority** Article 53(1) requires that each member of their supervisory authority (which in the case of the UK, is the Information Commissioner) be appointed by means of a transparent procedure be it by their parliament, their government, their Head of State; or an independent body entrusted with the appointment under Member State law.	The recruitment process for the UK Information Commissioner is conducted by a Selection Panel appointed by Government in accordance with the Commissioner for Public Appointments Code 2012. For the most recent appointment, the Selection Panel decided on the final two candidates for interview by relevant Government Ministers and the Public Appointments Assessor. The Government's preferred candidate gave evidence at a pre appointment hearing by the Culture Media and Sport Select Committee which currently has responsibility for information rights

	.	law. This process was first adopted by the Justice Committee in February 2011 *"as part of wider* measures to strengthen the independence of the Office of the Infor*mation Commissioner"* and is in line with the July 2007 Green Paper: The Governance of Britain which proposed that where Parliament has a particularly strong interest in a public post, the relevant select committee should hold a pre-appointment hearing for the government's preferred candidate. This open recruitment process and parliamentary oversight with the final appointment made by the Crown, appears to satisfy the criteria in Article 53(1). The independence of the Information Commissioner for data protection may further be measured by the resources it has to undertake this role. Currently the Information Commissioner receives 100% of the income from notification fees. As the notification requirement ceases to apply under GDPR, the Digital Economy Bill now includes provision, subject to regulations, for introducing a new funding regime but it is notable that the income generated will be collected by the Information Commissioner and paid into the Consolidated Fund which arguably undermines the independence of this role. This is perhaps of greater relevance after the UK withdraws from the EU assuming that once the UK is a "third country" the Government decides to seek an 'adequacy' determination from the EU Commission
Article 54	**Rules on the establishment of the supervisory**	None

	authority This Article sets out the qualifications and eligibility conditions, rules and procedure of appointment, duration of the term, reappointment eligibility and conditions governing obligations of members of the supervisory authority.	
Article 58 Recital(s) 129	**Powers** Article 56 (1) – (3) provides for the investigative, corrective and authorisation and advisory powers of the supervisory authority. The corrective powers in Article 58(2)(i) make clear that the supervisory authority must be able to impose an administrative fine pursuant to Article 83 instead of or in addition to the other measures outlined in Article 58(2). Article 56(6) provides that Member States may make provision for the supervisory authority to have additional powers to those in paragraphs (1), (2) and (3) provided that the exercise of those powers does not impair the effective operation of Chapter VII (cooperation and consistency between supervisory authorities).	If the Government is minded to propose the supervisory authority has additional powers it would be helpful to understand what these powers are and the reason for them. It is worth observing that civil monetary penalties are already higher than the fines imposed on those convicted of s.55 offences under the DPA for obtaining or procuring personal information unlawfully. Attempts to align the civil and criminal sanctions have failed as the custodial penalties provided for in s.77 of the Criminal Justice and Immigration Act 2008 for the unlawful obtaining of personal information have not been brought into effect. In the intervening period, there has been a piecemeal approach to introducing criminal offences, sometimes including custodial sentences (most recently in the Digital Economy Act 2017) but these are not directed at external criminals deliberately misusing personal

		information for their own benefit, including financial gain but rather used as a means of providing assurance that adequate sanctions and safeguards are in place to support increased data sharing. Whilst all controllers must strive to ensure their data protection practices and security standards are compliant, there is a serious mismatch between the penalties faced by controllers and/or their employees with those available to the ICO/CPS when serious data protection crimes are committed and this needs to be addressed to restore public trust and confidence. Custodial penalties are perceived as deterrents for other offences and serious data protection crimes should be regarded in the same way.
Article 59	**Activity reports** This Article requires that each supervisory authority shall draw up an annual report on its activities which must be transmitted to: - the national Parliament and the government and such other bodies as are designated by national law - the public, the Commission and the European Data Protection Board (EDPB)	Member States have discretion to determine whether the report includes a list of the type of infringements notified and nature of measures taken in accordance with Article 58(2) (corrective powers/measures). The Information Commissioner already publishes some information about enforcement measures on a case by case basis. Notwithstanding this, in the interests of openness, transparency and parliamentary scrutiny we consider that the UK supervisory authority should be required to include such a list in its annual activity report and that this list should be comprehensive save any

		circumstance where publication would or would be likely to prejudice national security. This will also provide confidence and assurance that a consistent approach is taken across all sectors.
Article 62 Recital 134	**Joint operations of supervisory authorities** This Article requires supervisory authorities, where appropriate, to conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other Member States are involved and sets out the legal framework for these types of operations. Article 62(3) provides for staff from one supervisory authority to be seconded to another MS lead authority and for the conferral or powers, including investigative powers on the seconded staff by the host supervisory authority for the purposes of joint operations but only to the extent that Member State law provides for this.	Having no direct knowledge of the extent to which such measures may or may not be required, we have not made comment on this discretionary provision.
Article 90 Recital 164	**Obligations of Secrecy** This Article provides for Member State law to place limitations on the operation of the supervisory authority's powers to obtain access/information from controllers and/or processors in order to safeguard professional or	Under the Data Protection Act 1998, provision is made for the necessary protection of legally privileged information in the context of the exercise of enforcement powers by the Information Commissioner. See by way of example:

	other equivalent secrecy obligations in so far as this is necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy.	• s.41(B) (3) & (4), Assessment Notices: Limitations, • s.43 (6) & (7) Information Notices; • s.44 (7) & (8) Special Information Notices; Similar safeguards need to be provided for exclusions from the information disclosure obligations of controllers and processors to the supervisory authority in the context of the GDPR.
2. Sanctions		
Article 36 Recital 94, 95, 96	**Prior consultation** Under Article 35(1) where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller is required before processing commences to conduct an assessment of the impact of the envisaged processing operations on the protection of personal data. Article 36(1) places an additional duty on the controllers to consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the **absence of measures** taken by the controller to mitigate the risk.	Notwithstanding Article 36(1), paragraph (5) provides that Member State (MS) law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health. The above processing types will probably relate solely or predominantly to processing undertaken by public authorities and public bodies. It is clear that this type of processing given its sensitivity is more than likely to engage Article 35(1) in any case and, where appropriate, trigger the obligation in Article 36(1). Imposing an additional requirement under domestic law to require prior consultation with the supervisory

		authority for certain categories of processing undertaken by public authorities, therefore does not appear to be either necessary or desirable.
Article 58 Recital 129	**Powers**	See above comments in relation to Article 58
Article 83 Recital 148, 150, 151	**General conditions for imposing administrative fines** Article 83 sets out the general conditions for imposing administrative fines. Article 83(7) provides discretion for each Member State to lay down rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.	This discretion should be exercised in the UK to ensure that administrative fines in respect of public authorities are no higher than the maximum financial penalties currently applicable under the Data Protection Act 1998 and Data Protection (Monetary Penalties) (Maximum Penalty and Notices Regulations 2010/31, with clarity as to the implications for external organisations (when acting as controllers or processors) in the supply chain. Such fines are paid into the Treasury's Consolidated Fund. If the fines applicable to public authorities and public bodies are not limited in this way and are set at the levels specified in Article 83, then the discretion in Article 83(9) should be exercised to ensure that all fines are imposed by a competent national court. Article 83(5) sets out the nature of the infringements that are subject to administrative fines up to 20,000,000 EUR or in the case of undertakings 4% of

		total worldwide annual turnover. Paragraph (5)(d) includes any obligations pursuant to Member State law adopted under Chapter IX (provisions relating to specific processing situations - where member states have the discretion to determine their own rules). Article 83(8) requires the exercise by the supervisory authority of its powers under this Article to be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process and therefore if the supervisory authority is to impose fines directly then we would expect that, as now, this will be subject to judicial remedy.
Article 84 Recital 149, 152	**Penalties** Article 84 requires Member States to adopt rules on other penalties applicable for infringements of the regulation, including those that are not subject to administrative fines under Article 83 and that such penalties must be effective, proportionate and dissuasive.	As in relation to Article 58 (powers) if the Government is minded to propose the supervisory authority adopts rules on penalties beyond those in the Regulation it would be helpful to understand what these are and the reason for them. Also see comments on Powers (Article 58)
3. Demonstrating Compliance		

Article 40 Recital 98, 99	**Codes of Conduct** Article 40(1) place an obligation on Member States, the supervisory authorities, the EDPB and the Commission to encourage the drawing up of codes of conduct intended to contribute to the proper application of the Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises. The subsequent paragraphs outline: - which types of bodies may be involved in preparing the Codes (Art 40(2)) - the scope and topics that may be included in the Codes (Art 40(2)) - the approval process for Codes in respect of processing activities confined to a single Member State (Art 40(5)) - the approval process for Codes in respect of processing activities involving multiple Member States (Art 40(7)) - the mechanism for mandatory monitoring of compliance by accredited bodies (Art 40(4)) - publicity for, publication and registers of approved Codes (Art 40(10,11) - scope for third countries who are not subject to the GDPR to adhere to Codes as part of framework for demonstrating safeguards (Art 40(3))	It would be helpful if Government and the ICO set out their views on how this obligation is to be met.

Article 42 & Article 43 Recital 100	**Certification & Certification Bodies** These Articles provide for data protection certification mechanisms and data protection seals and marks to enable controllers and processors to demonstrate that their processing operations are compliant with the Regulation.	As with Article 40 above, it would be helpful if the Article 29 Working Party (soon to become the European Data Protection Board – EDPB) and the ICO set out their views on how certification bodies are to be accredited and when these certification mechanisms are likely to be available.
4. Data Protection Officers		
Article 4 Recitals 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37	**Definitions** There is no definition in Article 4 relating directly to Data Protection Officers. Article 4(7) defines a 'controller; as meaning a 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. It also states that: *"where the purposes and means of such* processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or *Member State law"* **Comment:** This provide Member States with the discretion to determine who constitutes a controller.	Further explanation of exactly which category of public authorities or functions are in scope and the implication of not being regarded as a 'recipient' for individual disclosures would be helpful. If it is the case that individual schools as public authorities must designate a data protection officer, then it would be helpful if DfE informed schools of this as a matter of urgency. (reference should also be made other comments around school status eg maintained, academy, trust)

	In Article 4(9) a '**recipient**' is defined as a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. It also states that: *".. public authorities which may receive personal* data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection *rules according to the purposes of the processing"* Recital 31 provides additional context. The gist of this means that where a case by case inquiry is made by a certain category of public authority under an express legal requirement for the exercise of their official mission, the receiving public authority will not be regarded as a 'recipient'.	
Article 37 Recital 97	**Designation of the data protection officer** Article 37(1) requires controllers and processors to designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the **core activities** of the controller or the processor consist of processing operations	Article 37(4) provides that Member State law may require the designation of a data protection officer over and above the requirement specified in paragraph 1. As public authorities are subject to the mandatory requirement irrespective of size, we do not consider it appropriate to comment on the domestic extension of this requirement to bodies not otherwise prescribed under the GDPR.

	which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10	
Article 38 Recital 97	**Position of the data protection officer** Article 38(5) provides for Member State law to impose secrecy/confidentiality requirements on data protection officers.	Given the tasks of the data protection officer in Article 39(1)(d) & (e) specifically in relation to the supervisory authority, clarity over the scope of secrecy/confidentiality obligations is needed in this area.
5. Archiving & Research		
Article 89 Recital 156, 157, 158, 159, 160, 161, 162, 163	**Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes** Article 89(2) & (3) provide for Member States to disapply the rights of individuals. Where the processing is for scientific or historical research or statistical purposes the rights in Articles 15 (subject access), 16 (right to rectification), 18	We support derogation from the application of the above rights in these limited circumstances.

	(restriction of processing) and 21 (right to object) may be disapplied subject to observing the conditions and safeguards in Article 89(1) in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes and are necessary for the fulfilment of these purposes. Where the processing is for archiving purposes in the public interest, Member State law may provide derogations from the rights in Articles 15, 16, 18, 19 (communication of restriction or erasure to recipient) and 21 subject to the same conditions and safeguards as above.	
6. Third Country Transfers		
Article 49 Recitals 111, 112, 113, 114, 115, 116	**Derogations for specific situations** Article 49(1) sets out the conditions which must be satisfied for transfers to third countries in the absence of an 'adequacy' determination under Article 45(3) or appropriate safeguards pursuant to Article 46. Other than where: • the data subject explicitly consents; • the transfer is for the establishment, exercise or defence of legal claims; • the performance or conclusion of a contract	In both instances referred to, provision must be made in MS law for transfers to third countries. Obviously once the UK withdraws from the EU it will more than likely be itself regarded as a third country.

	in the interest of the data subject; • vital interests (physical integrity or life); the other conditions specified for such transfers are where: • the transfer is necessary for important reasons of public interest (Article 49(1)(d) (recognised under MS law (Article 49(4)) which may also set limits on specific categories of personal data to be transferred to third countries (Article 49(5)) • the transfer is made from a register established under MS law and subject to conditions laid down in MS law in (Article 49(1)(g)) Recital 112 addresses what may constitute important reasons of public interest giving the following examples for cases of international data exchange: • between competition authorities, • tax or customs administrations; • between financial supervisory authorities; • between services competent for social security matters; or • for public health, for example in the case of contact tracing for contagious diseases or • in order to reduce and/or eliminate doping in	

	sport • international humanitarian law applicable in armed conflicts (both public and vital interest of data subject (recital 112)) • compelling legitimate interests pursued by the controller, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller has assessed all the circumstances surrounding the data transfer (recital 113) In the case of registers, recital 111 clarifies that such a transfer should not involve the entirety of the personal data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or, if they are to be the recipients, after taking into account the interests and fundamental rights of the data subject.	
7. Sensitive Personal Data and Exceptions		
Article 9 Recitals	**Processing of special categories of data** Article 9(1) prohibits the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade	Even where the data subject has given explicit consent to the processing of special category data (SCD), Article 9(2)(a) provides discretion for MS law to restrict

51, 52, 53, 54, 55, 56	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 prohibition may be set aside where a specified condition in Article 9(2) is satisfied.	the lifting of this prohibition. The conditions specified for setting aside the prohibition on processing SCD other than with the explicit consent of the data subject are: • for employment and social protection purposes under (Article 9(2)(b)) • for reasons of substantial public interest (Article 9(2)(g)) • for the purposes of preventive or occupational medicine, for the assessment of working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services (and also by a professional subject to an obligation of professional secrecy under MS law (Article 9(2)(h) • for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices (Article 9(2)(i)) • for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 83(1) (Article 9(2)(j)) or • for further conditions and limitations with regard to the processing of genetic,

		biometric or health data (Article 9(4)) These are all subject to Member State law, and to adequate safeguards. This could be achieved by introducing provisions similar to those in the The Data Protection (Processing of Sensitive Personal Data) Order 2000/417. Clearly such measures are vital in ensuring that the GDPR contains adequate safeguards and exemptions to ensure the necessary, justified and proportionate use and disclosure of SCD.
8. Criminal Convictions		
Article 10	**Processing of personal data relating to criminal convictions and offences** Processing of personal data relating to criminal convictions or offences or related security measures under Article 6(1) must be carried out under the control of official authority or where authorised by MS law, subject to provision of adequate safeguards.	This could be achieved by introducing a similar exemption to the crime and taxation provision applicable under s.29(1) and (3) of the DPA and similar grounds to those in The Data Protection (Processing of Sensitive Personal Data) Order 2000/417 provided adequate safeguards apply.
9. Rights and Remedies		
Article 17	**Right to erasure ("right to be forgotten")** The data subject's right to the erasure of personal data by the controller applies where one of the	Article 17(1)(e) provides for erasure where this is for compliance with a legal obligation in Member State law

Recitals 65, 66	following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).	to which the controller is subject. This right does not apply where processing of personal data is required for compliance with a legal obligation by Member State law for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller and for this reason it seems the right of erasure is unlikely to apply to public authorities other than where consent is relied on as the legal basis for processing.
Article 22	**Automated individual decision-making, including profiling**	This provision does not apply if the decision is authorised by Member State law and this also lays down suitable measures to safeguard the data

Recitals 71, 72	Article 22 provides the right of the data subject not to be subject to automated individual decision making, including profiling.	subject's rights, freedoms and legitimate interests. It would be helpful to know whether Government intends to legislate in this area.
Article 26 Recital 79	**Joint controllers** Article 26(1) enables Member State law to determine the responsibilities of joint data controllers.	It would be helpful to know whether Government intends to legislate in this area or intends to rely on statutory guidance issued by the supervisory authority.
Article 80 Recital 142	**Representation of data subjects** Article 80(2) allows Member States to introduce the legal right for data subjects to be represented by a properly constituted (in law) not for profit organisation or association (active in privacy rights) in terms of lodging complaints or exercising the rights on behalf of one or more data subjects under Articles 77, 78 and 79, including exercising the right to seek compensation referred to in Article 82 if it considers that the rights of a data subject have been infringed by non-compliant processing.	FoIA applicants are supported by the Information Commissioner in seeking a legal remedy e.g. to complain against refusal to grant access to official information. Currently the Information Commissioner does not assist data subjects in seeking financial redress on an individual basis but undertakes assessments in response to complaints received and may take enforcement action against a controller in breach of its legal obligations. Whether 'not for profit' organisations active in information rights should have the legal right to support an individual or multiple individuals in bringing claims for compensation against controllers is a policy matter for government to determine.

10. Processing of Children's Personal data by On Line Services		
Article 8 Recital 38	**Conditions applicable to child's consent in relation information society services** Where consent is required in relation to the offer of information society services[1] directly to a child, this will only be valid if the child is below the age of 16 years where that consent is given by the holder of parental responsibility over the child. (This does not extend to preventative services and counselling which young people under 16 are eligible to access without parental consent).	Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years. The definition of information society services refers to any service 'normally' provided for remuneration at a distance, by electronic means and at the individual request of the recipient of the service. Unless this applies to social media which is free at point of use (though often subject to behavioural advertising), it appears that as public authorities are not providers of on line information society services aimed specifically at children, this provision is unlikely to apply. We are aware that age verification for access to adult pornographic material is being introduced in the Digital Economy Act (which received Royal Assent on 28/4/2017.

[1] The full definition of "information Society Service" is taken from Article 1 (1)(b) of Directive 2015/1535 which says:

(b) 'service' means any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.
For the purposes of this definition:
(i) 'at a distance' means that the service is provided without the parties being simultaneously present;
(ii) 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means;
(iii) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request.

		In the context of subject access rights, the ICO anticipates that a case by case determination is made to assess the maturity and understanding of a young person under 16. This is not a feasible approach in the on line environment. For child protection and safeguarding reasons local authorities have understandable concerns about the risks children face when accessing the internet and social media sites without parental supervision. Imposing the requirement for parental consent for children under a specific age must be capable of enforcement and to be effective must be accompanied by greater public education and awareness of the parental filters, privacy settings and security measures available to help children stay safe on line.
11. Freedom of Expression in the media		
Article 85 Recital 153	**Processing and freedom of expression and information** Article 85 provides for MS law to reconcile right to protection of personal information with the right to freedom of expression and information and for MS to determine exemptions from: Chapter II – principles; Chapter III – rights of the data subject;	Section 32 of the DPA 1998 provides significant exemptions for journalistic (and other related purposes) from compliance with all but the 7th principle and many existing data subject rights where the controller holds a reasonable belief publication would be in the public interest (this amended provision was brought into effect to remove risk of custodial sanctions provided for in s.77 of the Criminal Justice and Immigration Act 2008 in respect of the unlawful obtaining of personal information but this sanction has not been brought into

	Chapter IV – controller and processor; Chapter V – transfer of personal data to third countries or international organisations; Chapter VI – independent supervisory authorities; Chapter VII – cooperation and consistency; and Chapter IX – specific data processing situations if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.	force). Other provisions also limit the civil enforcement measures the supervisory authority is able to pursue. Whilst recognising the importance of journalistic freedoms in a democratic society, any extension of the current exemptions as a consequence of the GDPR for freedom of expression purposes should be subject to intense public scrutiny in the light of the findings in the Leveson Inquiry.
12. Processing of Data		
Article 6 Recitals 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50	**Lawfulness of processing** Article 6(1) sets out the grounds which must be satisfied to lawfully process personal data. These grounds are where the processing: a) relies on the consent of the data subject; b) is necessary for entering into or the performance of a contract; c) is necessary for compliance with a legal obligation to which the controller is subject d) is necessary in order to protect the vital interests of the data subject or of another natural person e) is necessary for the performance of a task carried out in the public interest or in	There is no one single source of law that governs the use, sharing/disclosure and retention of personal information by public authorities. Local authorities are creatures of statute and must have “vires” established in legislation. Even if the vires exists, this must be exercised lawfully in compliance with legal obligations under the common law and statute, including the transparency, necessity and proportionality requirements in the DPA 1998 and the Human Rights Act 1998. Public authorities require clarity as to whether general powers provide the necessary degree of legal precision and certainty or whether Article 6 necessarily means

	the exercise of official authority vested in the controller f) is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child (does not apply to processing undertaken by public authorities in performance of their tasks) Article 6(2) provides that Member States may maintain or introduce more specific provisions to adapt the rules with regard to processing for compliance with points (c) (processing necessary for compliance with a legal obligation) and (e) (processing necessary for performance of a task carried out in the public interest or in the exercise of official authority vested in the controller) by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX. Article 6(3) provides that processing for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	that the processing must support a clearly defined and foreseeable purpose in line with the express or implied statutory functions of the relevant public authority in pursuit of a justified, proportionate and legitimate aim. Furthermore the secondary use of personal data under the GDPR is more exacting than under the DPA 1998. Under the DPA 1998 secondary use is permitted provided this is not incompatible with the original purpose whereas under the GDPR, it is necessary to show that secondary use is compatible with the original purpose. For these reasons it would be useful for UK law to clarify the rules and circumstances when controllers may rely on sub paragraphs (c) and (e).

	must be laid down by MS law. The MS law must meet an objective of public interest and be proportionate to the legitimate aim pursued. Rectal 41 makes clear that where the GDPR refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned but that such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the 'Court of Justice') and the European Court of Human Rights.	
Article 18 Recital 67	**Right to restriction of processing** Article 18(1) provides the right for the data subject to require the controller to restrict (quarantine) processing on a number of grounds. These grounds include where: • the accuracy of the data is contested; • the processing is unlawful; • the data is no longer needed save for legal claims of the data subject, or • the legitimate grounds for processing are	If the Government is minded to legislate in this area it would be helpful to understand what is being proposed and the reasons for this.

	disputed Article 18(2) provides that this right may be over-ridden *"for reasons of important public interest of the Union or of a Member State"*	
Article 28 Recital 81	**Processor** Article 28(3)(a) & (g) require controllers to ensure that processing of personal data by a processor acting for them is governed by a binding legal contract which amongst other requirements, specifies that the processor must only act on the written instructions of the processor and the arrangements for the deletion or transfer of the data once the provision of services ends. Member State law can introduce legislation binding data processors and/or require the transfer and storage of data, overriding the instructions of a controller.	If the Government is minded to legislate in this area it would be helpful to understand what is being proposed and the reasons for this.
Article 29	**Processing under authority of the controller and processor** The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process	If the Government is minded to legislate in this area it would be helpful to understand what is being proposed and the reasons for this.

	those data except on instructions from the controller. Union or Member State law can override the processing instructions from the controller or processor.	
Article 32 Recital 83, 74, 75, 76, 77	**Security of processing** Article 29(4) requires both the controller and processor to take steps to ensure that personal data is only processed on the instructions of the controller. However, Member State law can override the processing instructions from the controller or processor.	If the Government is minded to legislate in this area it would be helpful to understand what is being proposed and the reasons for this
Article 35 Recital 75, 84, 89, 90, 91, 92, 93	**Data Protection Impact Assessment** Article 6(1) Includes the following conditions in relation to the lawful processing of personal data: (c) processing is necessary for **compliance with a legal obligation** to which the controller is subject; (e) processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller; Where processing pursuant to Article 6(1) (c) or (e) has a legal basis in Union law or in the law of the	In our view Government should not require public authorities to undertake a further DPIA if this has already been undertaken for the same or similar processing activity/activities in question if such an assessment has been undertaken for that specific processing activity when the legal basis was adopted. The regulator should provide a standard secure online form for any DPIA and also outline their performance standards for assessing. It may be practical again to see where through “data devolution” activities city

	Member State to which the controller is subject and that law regulates the specific processing operation or set of operations in question, under Article 35(10) the requirements in paragraphs 1 to 7 do not apply where a data protection impact assessment has already been carried out as part of a general impact assessment at the time the legislation is introduced, unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.	regions are given some limited powers to support this work which will more than likely be onerous for the ICO.
Article 37 Recital 97	**Designation of the Data Protection Officer**	See above comment in relation to Article 37(4)
Article 86 Recital 154	**Processing and public access to official documents** Article 86 provides that personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject.	This reconciles public access to official documents with the right to the protection of personal data and leaves Member State law to strike this balance. At present the Freedom of Information Act 2000 amends the Data Protection Act 1998 and provides the framework for undertaking this balancing exercise with disclosures of personal data in response to public access requests considered under DPA Schedule 2, condition 6 (legitimate interests). The legitimate interest ground is a processing condition public authorities may no longer rely on in the performance of their tasks so presumably this

		particular ground is not available for disclosure of personal data under public access legislation. If that is the case then legislative measures will be needed to ensure that there is a framework that enables public authorities to strike a balance between the interest of requesters and the protection of individual privacy rights when considering access requests involving personal information.
Article 87	**Processing of the national identification number** Article 87 provides for Member States to further determine the specific conditions for the processing of a national identification number or any other identifier of general application subject to appropriate safeguards for the rights and freedoms of the data subject.	This requires Member States to set out the framework for the use and disclosure of national identification numbers or other common identifiers such as the NHS number for direct care purposes (as provided for in S251A of the Health and Social Care Act 2012 as inserted by S.2 of the Health and Social Care (Safety and Quality) Act 2015). If the Government is minded to further legislate in this area it would be helpful to understand what is being proposed and the reasons for this
Article 88 Recital 155	**Processing in the context of employment** Article 88(1) provides discretion for Member States (by law or collective agreements) to introduce more specific rules to ensure the protection of rights and freedoms in respect of the processing of employee's personal data in the employment context, including specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights.	If the Government is minded to legislate in this area it would be helpful to understand what is being proposed and the reasons for this.

13. Restrictions		
Article 23 Recital 73	**Restrictions** The UK can restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34 (data subject notification of breach) as well as Article 5 (principles) in so far as such measures correspond to the rights and obligations provided for in Article 12-22. Restrictions must respect the essence of fundamental rights and freedoms and be a necessary and proportionate measure. This allows for relaxation of obligations and/or disapplication of rights for the following purposes: (a) national security; (b) defence; (c) public security; (d) 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; (e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security; (f) the protection of judicial independence and	The scope of Article 23 effectively enables member States to provide for similar exemptions to those now applicable under the Data Protection Act 1998 (DPA) in Sections 27—31, 34 – 35 and some or all of the exemptions in the miscellaneous exemptions category in Section 37, fully set out in Schedule 7. In relation to section 30 the Secretary of State has introduced the following orders in respect of health, education and social work: • The Data Protection (Subject Access Modification) (Health) Order 2000/413 • The Data Protection (Subject Access Modification) (Education) Order 2000/414 • The Data Protection (Subject Access Modification) (Social Work) Order 2000/415 The Data Protection (Miscellaneous Subject Access Exemptions) Order 2000 also exempts from subject access personal data the disclosure of which is prohibited or restricted by certain enactments and subordinate instruments in the interests of safeguarding the interests of the data subject himself or the rights and freedoms of some other individual. (This relates to the rules applicable to adoptions and information about human fertilisation and embryology for example). It is clearly sensible to adopt similar exemptions in the

	judicial proceedings; (g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions (h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g); (i) the protection of the data subject or the rights and freedoms of others; (j) the enforcement of civil law claims Legislative measures must contain specific provisions as listed in Article 23(2).	context of the GDPR provided that the restrictions are necessary and proportionate and adequate safeguards apply.
14. Rules surrounding churches and religious associations		
Article 91 Recital 165	**Existing data protection rules of churches and religious associations**	No further comments.
15. Additional questions – cost impact		
None	**In context of derogations above, what steps should the Government take to minimise the cost or burden to business of GDPR?**	Government should ensure that any replacement fees for loss of notification income to be introduced as a result of amendments to the DPA 1998 (to be inserted if Digital Economy Bill is enacted) are not excessive for larger data controllers who may in any case incur significant additional costs if subject to the criteria for the mandatory appointment of a Data Protection Officer (DPO).

		The mandatory requirement for a DPO appears to apple irrespective of the size of a public authority (although large scale processing maybe a consideration) and this is likely to impose a significant burden on schools who are unlikely to have 'in house' data protection expertise or budget. The complexity of the range of different types of schools eg maintained schools, Academies and School Trusts also means that a 'one size fits all' is neither sensible or appropriate. DfE/ ICO do need to provide clarity as a matter of urgency on this. It should also be made clear of any duty of care expectations on that LA if the school is maintained. In terms of mitigating the burden of GDPR compliance clarification/confirmation of the following issues would be helpful: • the extent and level of record keeping requirements at corporate level to demonstrate overview and control of processing activities • standard GDPR compliant contractual clauses issued by Office of Government Commerce (OGC)/Crown Commercial Service (CCS) for inclusion in public sector data processor contracts. The designated DPO role will result in greater costs for data controllers that are required to have a designed DPO.

		Although the role will be invaluable in supporting compliance around how personal information is managed and processed, the average cost to train and keep the officer skills up-to-date will be around £4k (every few years) when the total costs are factored. Any data devolution to city regions needs to provide some local flexibility in relation to these regulations so that these areas can use personal data for appropriate, fair and lawful purposes, and in doing so provide the services required. This will be particularly important around health and social care. Overall nationally Government should set out how this regulation can be effectively used to support service delivery and better overall access and management of personal data.