Hope Kindness Forgiveness Aspiration Love Courage Trust Respect Friendship

Drake Primary School and Little Pirates Child Care

DATA PROTECTION POLICY

Formally adopted by the Governing Board of:-	**Drake Primary School & Little Pirates Child Care**
Chair of Governors:-	**Ann Morgan**
Created on:-	**April 2023**
Brought to Governors & adopted on:-	

Drake Primary School and Little Pirates Childcare, where a world of opportunities awaits

Our school and curriculum must reflect the world: past, present and future, in all its diversity.
We unlock opportunity and inspire everyone.

We aim to provide:

- a school where learning is visible and children are safeguarded and nurtured
- a rigorous assessment system to ensure no pupil falls behind
- a diverse learning community where pupils, families and staff collaborate to refine practice and develop positive and rewarding relationships
- a workplace where staff contribute to professional learning communities; locally, nationally and globally.

So our mission is to:

- inspire the poets, geneticists and astronauts of the future
- ensure children are happy and healthy through our values and play
- develop a culture where reading for pleasure is for everyone
- make the arts a central component for children's lifelong learning
- build a curriculum of joy and curiosity

Executive Headteacher: Mrs Louise Rosen
Drake Primary School and Little Pirates Child Care, Fairfields, Thetford, Norfolk, IP24 1JW Tel: (01842) 762055

office@drake.norfolk.sch.uk www.drake.norfolk.sch.uk

Table of Contents

Introduction 3
GDPR and the Data Protection Act 2018 3
Data protection principles and GDPR principles 4
1. Accountability principle 5
2. Processing and consent 5
3. Privacy/information notices 6
4. Special categories of personal data (was sensitive personal data) 6
5. Individual rights and legal basis for processing 7
6. Data subject access requests (right of access) 9
7. Requests for erasure and withdrawing consent 10
8. Data portability 10
9. Automated decision-making 11
10. Retention and storage limits 11
11. Third parties – data processors 11
12. Data transfers outside the EEA 12
13. Privacy impact assessments (PIA) 12
14. Reporting of breaches/Sanctions 12
15. Data Protection Officer (DPO) 13
16. Training 13
Appendix 1 – Information/privacy notices 14
Appendix 3 – Examples of automated decision making 16
Appendix 4 – Table of changes 17

Data Protection Act 2018 and GDPR

Introduction

This document outlines what the GDPR and Data Protection Act (DPA) 2018 are and how they impact, in an HR context. NB. There are other implications of the GDPR and DPA 2018, for schools and academies to consider beyond HR considerations e.g. ICT systems, pupil data etc

GDPR and the Data Protection Act 2018

GDPR is the new legislation which governs the collection and processing of personal data in the EU. It is designed to strengthen and unify the safety and security of all data held within an organisation. The GDPR was enacted in May 2016 and all EU countries (including the UK) were given a grace period of 2 years to ensure they were compliant for 25 May 2018, when the regulations came into force. Any organisations not compliant risk facing penalties. The GDPR are EU regulations and will apply, despite Brexit.

GDPR gives member states (including the UK) a number of opportunities to make provisions for how it applies in their country (immigration, criminal records and details of enforcement provisions). The DPA 2018 details these. It is therefore important that the GDPR and DPA 2018 are read alongside each other. The DPA 2018, replaced the Data Protection Act 1998

The GDPR requires a much stricter compliance regime. There are several new concepts, approaches to data and restriction on processing. It also expands rights for data subjects and significantly increases sanctions. GDPR aims to balance the requirement to process data without impeding individual rights. In an HR context, the GDPR and DPA 2018 regulates the processing of employee data.

The GDPR applies to personal data[1]. This includes:

- information in an employee's personnel file
- information held on HR systems
- information contained in emails
- information obtained through employee monitoring
- information on prospective job applicants
- information on contractors

NB. It doesn't just relate to employees and workers, it is identifiable personal data relating to any individuals the data controller (see below) is collecting information on. It is important to note that the GDPR relates to both electronic records and paper records, but only paper files that are filed in a structured way. There is ICO guidance on this but a general rule to follow is the 'temp test'. This is to consider if on a temp's first day you asked them to find information on a specific person within the paper filing system, would they be able to find it without having to ask colleagues for help? If yes, then it is a structured filing system.

The GDPR will regulate the **processing** of this data, including the:

- collection
- storage
- use
- alteration
- disclosure
- destruction

Schools and trusts are **data controllers** because they are organisations that collect personal data.

Employees and job applicants will be **data subjects** because they will be individuals to whom the data relates. Schools and academies are also likely to be **data processors** as they may process personal data for third parties.

Educator Solutions HR Services will be **data processors** for its customers.

[1] Personal data – 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (ICO).

Data protection principles and GDPR principles

The GDPR principles are largely similar to the previous data protection principles. Please see below: Data protection principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
   (a) at least one of the conditions in Schedule 2 is met, and
   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

GDPR Principles – 6 principles to ensure that data is *(italics show where the principle differs from the previous DPA 1998)*:

1. Processed fairly, lawfully and in a *transparent manner*
2. Used for specified, explicit and legitimate purposes and *not further processed in manner incompatible with those purposes* (Purpose limitation)
3. Used in a way that is adequate, relevant and *limited to what is necessary (*Data minimisation)
4. Accurate, kept up to date and, *if inaccurate must be erased or rectified without delay*
5. Kept no longer than is necessary *for the purposes of processing (*Storage limitation - retention)
6. Processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage, *using appropriate technical or organisational measures* Integrity and confidentiality (security)

What has changed?

This section details the changes and what impact it has:

1. Accountability principle

This was one of the biggest changes – Not only do organisations have to be compliant but they have to also demonstrate their compliance. Privacy by design is an express legal requirement under GDPR. Schools and trusts should embed the GDPR principles into all that they do e.g. compliance information in policies, GDPR principles carried out for all projects/initiatives/technology and systems which deal with personal data. This should all be evidenced too. The regulations include a requirement for organisations to keep extensive internal records of data processing operations, which must be shown to the ICO on request. Other requirements for compliance include:

- Create and maintain an up to date data risk register (schools and trusts with 250+ employees). The register must contain information about all personal data processed by the organisation (see appendix 2). Schools and trusts with less than 250 employees are required to maintain records or activities related to higher risk processing i.e. processing personal data which could result in a risk to the rights and freedoms of individuals or processing of special categories of data (see para 4) or criminal convictions and offences
- Undertake privacy impact assessments (PIA) for high-risk processing (see para 10)
- Implement measures to minimise risk of breaches
- Notify and keep a comprehensive record of data breaches[2](see para 11)
- Implement data protection by design and default – privacy by design. Consider it in all work carried out.
- Only process data which is required
- Designate a Data Protection Officer (DPO)[3](see para 15)

[2] A personal data breach means the destruction, loss, altering, unauthorised disclosure of or access to personal data. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, for example employees, data controllers must also notify them directly.

[3] A DPO must be appointed if the organisation is a public authority (this includes schools and trusts), or if the company carries out large scale systematic monitoring of individuals (e.g. online behaviour tracking) or the organisation carries out large scale processing of special categories of data or data relating to criminal convictions and offences.

2. Processing and consent

Under GDPR any processing of personal data must be able to be justified under a set number of legal basis', which organisations must be able to use to justify the processing. One of the legal basis' is consent. Where consent is used it must be 'freely given, informed, specific and explicit'. The implications of this is broad and general consents given in employment contracts to process employee data are no longer valid. NB. Educator Solutions HR Services produced contracts do not contain a requirement for consent. Consents must be kept separate and distinct from other terms and conditions. The data subject has the right to withdraw consent at any time. Additionally, if consent is given in a written declaration

that also concerns other matters the request for consent must be clear what it is being given for.

However, in an employer/employee relationship it will be quite difficult to deem consent as 'freely given' and therefore other grounds for processing must be relied upon. Additionally, where consent is given for processing the individual giving the consent has the right to be forgotten i.e. request all their data is erased. If this is the case, then the data can no longer be processed and may leave the school or trust unable to perform an important task. Therefore, using consent as grounds for processing could make processing difficult, so it is strongly advised that another legal basis is used (where possible) for processing. In an HR/education context, the other legal bases include that processing personal data is necessary:

- for compliance with a legal obligation –data is provided to payroll to provide statutory entitlements such as annual leave, maternity or sick pay
- for the performance of a contract –data is processed to pay employees or monitor employee attendance
- to carry out tasks in the public interest – salary and contract data is processed for staff because they are essential to educating children.
- For the purposes of the legitimate interest of the employer - Public authorities (including schools and trusts) can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority.

NB. There are other legal basis' for processing under the GDPR, which will apply to other personal data a school/academy processes e.g. pupil and parent data.

It is likely that most of the HR information in relation to school/trust staff will be processed under the existing grounds that the processing is necessary in relation to a contract or to carry out tasks in the public interest. Therefore, consent should have minimal impact.

Considerations

- Where any processing currently requires consent as the legal basis it may be worth considering if there is another legal basis that can be relied upon

- Ensure any consent given prior to the implementation of GDPR is given again. This is because the way in which existing consent is requested and therefore given means it is not likely to be GDPR compliant. Schools and trusts should record evidence of consent given.

3. Privacy/information notices

Data subject(s) need to be informed about what their data is being processed for, who is going to process it, how the data is collected and the legitimate aim for processing the data. This should be done in the form of an information/privacy notice (see appendix 1). Information/privacy notices should be published on the school/trust website so that they are easily accessible and they must be written in plain English. This must be done at the time the data is obtained (if directly from the individual or within one month if not directly from the original). This, basically, means the data subject must be made aware of the privacy notice either immediately or within one month. Only personal data that is necessary must be processed. Data subjects must be re-informed if the data is later processed for other purposes.

4. Special categories of personal data (was sensitive personal data)

Sensitive personal data is classified under Article 9 of the GDPR as racial or ethnic origin, political

opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health, sex life, sexual orientation.

Schools and trusts are likely to process most of this data and therefore need to demonstrate that they have a legal basis (as listed above) for processing the data **as well as one** of the following:

- Consent
- Necessary under employment law
- Necessary for legal proceedings
- Necessary to protect the vital interests of a data subject or another person
- Necessary to carry out tasks in the public interest
- Necessary for medical purposes
- Necessary for equal opportunities monitoring

There are separate safeguards for personal data relating to criminal convictions and convictions. Section 10 of the DPA 2018 details these. S.10 states that criminal conviction data can only be processed if it is allowed by member state law or under the control of an official authority. This requirement should not change anything for schools and trusts as DBS checks undertaken within schools and trusts are required by law.

5. Individual rights and legal basis for processing

Individuals have more rights under GDPR, but they do not apply in all situations. It will depend on the legal basis that the processing is being undertaken for.

The table below shows where the individual's rights apply, based on the legal basis the data is being processed under. If there is a 'x' then the right does not apply.

Individual right	**Legal basis for processing personal data**				
	Consent	**Performance of a contract**	**In the public interest**	**Compliance with a legal obligation**	**Defending a legal claim**
to rectification	X – except if inaccurate or incomplete	X – except if inaccurate or incomplete	X – except if inaccurate or incomplete	X – except if inaccurate or incomplete	X – except if inaccurate or incomplete

to be forgotten - erasure	Y	Y	X	X – except where the data must be erased to comply with a legal obligation	X
Objection to processing	X – but right to withdraw consent	X – except where the accuracy is being contested	Y – restriction on processing takes place whilst employer proves that their legitimate grounds for processing overrides those of the individual or that they are processing the data to defend a legal claim. Where there are no legitimate grounds the individual has the right to erasure.	X –except where the accuracy is being contested	Y – where employer no longer needs the informati on **and** the employee wants the data to establish, exercise or defend a legal claim.
Data portability	Y	Y	X	X	

NB. All the above individual rights apply where the personal data is unlawfully processed, and the processing is no longer necessary in relation to the purpose for which it was originally collected/processed.
If the personal data in question has been disclosed to any third parties, they must be informed of any changes to the data following an individual exercising their rights.

Data portability rights also apply where the personal data in question has been provided by the individual to the controller and where processing is carried out by automated means.

Where restrictions on processing are applied, because of objections to processing being raised be aware that it could cause significant delays to disciplinary and grievance procedures, redundancies and termination of employment.

Further information regarding the right to erasure and data portability can be found further on in the document.

6. Data subject access requests (right of access)

All individuals have the right to obtain confirmation that their data is being processed, have access to their personal data and be informed of what data is processed, how and why it is processed and who it is shared with. The GDPR builds on the previous data protection law by enhancing existing data subject rights and adding some new rights:

- Previous DPA law and now enhanced further – right to
  - o rectification
  - o access
  - o restrict processing
  - o object to processing

not be subject to automated decision making (including profiling)

- GDPR – right to
  - o transparency
  - o data portability
  - o erasure

Organisations are not allowed to charge under GDPR for a subject access requests (SAR) unless the request is 'manifestly unfounded or excessive'. Schools/trusts are not likely to be able to charge as requests are unlikely to fall within this definition.

Previously requests were required to be dealt with, within 40 calendar days. However, the GDPR requires requests to be dealt with within one month (at the latest or 3 months for complex requests). The one month time limit must be calculated from the day that the request is received (whether it is a working day or not) until the corresponding calendar date in the next month. If there is no corresponding calendar date in the following month, the date for responding will be the last day of that month.

The information required to be provided within data subject access requests has been extended under GDPR. Below shows what was previously required under data protection legislation and what GDPR has introduced (italics):

- The purposes of processing
- The categories of data processed
- The recipients, or categories of recipients (*in particular details of disclosure to recipients in third countries or to international organisations)*
- *The envisaged retention period, or the criteria used to determine this period*
- *The individual's rights of rectification or erasure, to restrict processing or to object to processing and to lodge a complaint to a supervisory authority.*
- *Information regarding the source of the data (if not collected from the data subject)*

- Details of any regulated automated decision taking *and the significance and envisaged consequences of the processing of the data subject.*

Considerations

Establish a procedure for dealing with and resolution of objections to processing of data and ensure staff know what a data subject access request is so that when one is received it is dealt with appropriately. NB. There is a specific exemption for a subject access request regarding references. See para 2.4 of *References: Provision to other employers' guidance G119* on InfoSpace for further information.

7. Requests for erasure and withdrawing consent

A data subject can request the deletion or removal of personal data where there is no compelling reason, or it's continued processing. Under previous data protection law the right to erasure was limited to processing that causes undue and substantial damage or distress. Under the GDPR this no longer exists but it provides several more circumstances where the right to erasure exists:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing processing
- The personal data was processed in breach of the GDPR
- The personal data must be erased in order to comply with a legal obligation

If the information has been disclosed to a third party, they must be informed. A request for erasure can be refused for several reasons. The ones which will apply in an HR context are as follows. The data is being processed:

- to comply with a legal obligation
- in the exercise or defence of legal claims

Considerations:

Ensure procedures are in place for dealing with rights of erasure requests.

8. Data portability

This was introduced under GDPR and is an enhanced form of data subject access. It allows data subjects to receive a copy of their personal data or have it transmitted to a third party in a safe and secure way and in a machine-readable format. This is more likely to apply to consumer situations e.g. using personal data to find a better car insurance deal. However, this could apply to an individual moving jobs. If a request is received the school or trust would have to provide the data requested electronically and in a commonly used format.

This right only applies to

- personal data processed by automated means
- personal data which the data subject has provided to the controller (i.e. excludes data obtained by the controller from other sources)

- where processing is justified on the grounds of consent or is necessary for performance of a contract

The information must be provided free of charge and within one month (two months for complex requests). If the request is refused the employer must explain why to the individual informing them of their right to complain to the ICO within one month.

Considerations:

Ensure systems would be able to provide information in the time frame required and to the required standards.

9. Automated decision-making

Data subjects have the right under GDPR not to be subject to a decision made solely by automated processing where that decision significantly affects them. However, there are exceptions to this rule. These are where automated processing is based on explicit consent or where it is necessary for entering into or performing the employment contract. If consent is used it may prove difficult to rely on because of the strict requirements relating to consent and proving that the processing is necessary for the contract.

For examples of where automated decision making may exist within HR see appendix 3.

Considerations:

Where automated decision making exists within a school or trust and the school or trust are not able to rely on an exception to the rule they must ensure employees are able to request human intervention, express a view on the processing and contest it.

10. Retention and storage limits

Schools and trusts should decide how regularly data should be reviewed to ensure it is up to date, accurate and still required. Any data that is found to be incorrect will need to be removed (unless there is another legitimate reason for holding it that the data controller/data processor can show that their legitimate interests for doing so override the interests or rights of the employee - or that

the purpose of processing is to establish or defend legal claims) See InfoSpace for a *model HR document retention schedule G320d*. Schools and trusts must ensure that retention periods are adhered to.

Considerations:

Ensure procedures for destroying data at the point the retention periods end are compliant with GDPR compliant and ensure storage of personal data is compliant with GDPR at all times.

11. Third parties – data processors

The GDPR applies to employers processing employee personal data (data controllers) and also applies to third parties who process employee personal data on behalf of the employer (data

processors). GDPR makes it a legal requirement for employers to choose data processors that have in place appropriate measures to meet GDPR requirements, demonstrated with formal contracts or SLA's.

Please see *Supplier contract statement G320c* on InfoSpace for Educator Solutions HR's demonstration of compliance, as a data processor for its customers.

Considerations:
Ensure any contracts schools and trusts have with third parties, who process employee personal data on their behalf, are GDPR compliant**.** Additionally, schools and trusts should ensure procurement procedures are reviewed to include due diligence on compliance measures.

12. Data transfers outside the EEA

Transfers of personal data outside of the EEA continue to be restricted under GDPR, although it was removed as a data protection principle. Countries that are already approved for personal data transfer remain so, so if any data transfers are taking place these can continue. Educator Solutions HR Services are unlikely to be affected by this as a data processor.

Considerations:
Ensure servers that host any systems, which hold personal data or back up personal data, are based in an approved country.

13. Privacy impact assessments (PIA)

Privacy Impact Assessments (PIA) are not new but what is new is that the GDPR expects them to be undertaken in certain cases. PIAs need to be carried out when planning a new initiative which involves "high risk" data processing activities i.e. where there is a high risk that an individual's right to privacy may be infringed such as monitoring individuals, systematic evaluations or processing special categories of personal data, especially if those initiatives involve large numbers of individuals or new technologies such as biometrics.
The idea behind a PIA is to identify and minimise non-compliance risks. The ICO has produced a Code of Practice on PIA's which helps guide through the process.

Considerations:
Ensure the requirement for these is built into planning for new initiatives and identify where they are required and undertake them.

14. Reporting of breaches/Sanctions

Under the previous DPA reporting of data breaches was not mandatory, under the GDPR they are. GDPR data breaches are deemed as:

'A data breach which leads to the destruction, loss, alteration, unauthorised disclosure of or access to personal data which, if unaddressed is likely to have significant detrimental effect on the individuals through:

- discrimination

- damage to reputation
- financial loss
- loss of confidentiality
- any other significant economic or social disadvantage'

If the breach is likely to be classed as high risk, then the data subjects must be informed.
Data breaches must be reported within 72 hours to the ICO (major breaches only). Sanctions for breaches are significantly higher and the worst offenders could receive fines of up to £17million or 4% of total worldwide annual turnover, whichever is higher. Sanctions could also include unlimited fines were criminal offences are committed[4]. Under the previous DPA enforcement rules applied to data controllers only. Under the GDPR enforcement rules apply to both data controllers and data processors.

The GDPR also makes it easier for individuals to bring private claims against data controllers, including past and present employers. Any damage an individual has suffered due to a breach could result in the right to receive compensation, including for distress and hurt feelings even where there is no financial loss. Employees or ex-employees (data subjects) could bring group actions via trade unions.

Schools and trusts who fail in compliance will see their Ofsted ratings being affected.

Considerations

Ensure all staff understand what a breach is and know what action to take.

15. Data Protection Officer (DPO)

Every school and academy is required to have a DPO, under the GDPR. The school or trust may decide to employ one, this could be one per trust, cluster etc. or the role could be accessed externally via a traded service (see 'Considerations' below). The tasks of a DPO are defined in s.69-71 of the DPA 2018. This role must report to the highest level of management within the school or trust (or group of schools or trusts) and operate independently. They cannot be dismissed or penalised for performing their task and must have adequate resources to enable them to carry out their duties. Consideration should be given to the resource and time required for the role when deciding who to appoint/allocate the tasks to.

Consideration:

Data Protection Officers can be secured as part of NCC's traded Information Management Compliance Solutions Service (IMCSS). There are model job descriptions for Data Protection Officers on InfoSpace *GR2499* and *GR005.*

[4] New offences have been created: Intentionally or recklessly re-identifying individuals from anonymised or pseudonymised data and altering records with intent to prevent disclosure following a subject access request.

16. Training

It is advised that all staff who have access to personal data should undertake mandatory data protection training. Staff more involved in data protection advice should receive further, enhanced training. Training should be refreshed on a regular basis.

Considerations:

- Decide who the training will be delivered by

- Keep records of who has received training and who has not
- Ensure data processors are aware of why they are processing the data

17. Other resources:

- DPA 2018 (Act in full)
- Data protection (gov.uk information)
- ICO's Guide to Data protection
- ICO's General Data Protection Regulations Guidance
- ICO's Privacy by design page

Appendix 1 – Information/privacy notices

Please see below for what should be contained in a GDPR compliant information/privacy notice:

- The name and contact details of the school/academy as a data controller
- The data protection officer's (DPO) contact details the purposes for which the data will be processed and the legal bases for processing, including, if relevant, the legitimate interests relied on
- The categories of personal data to be processed
- Details of any third parties the data will be shared with
- The recipients of the data
- Any transfer of the data outside the EEA
- The period of storage
- The rights of data subjects, including the right to access, rectify, erase data and the ability to withdraw consent or object to processing, and the right to lodge a complaint with the supervisory authority (ICO).
- The consequences for the data subject of failing to provide data necessary to enter into a contract (is there a legal obligation to provide the data)
- The existence of any automated decision-making and profiling and the consequences for the data subject

This information must be provided at the point of data collection. If a further requirement for processing transpires it must inform employees or job applicants of that requirement.

Gov.uk have produced sample privacy notices for schools to use. Please see here. There is a *Model Privacy notice for employees and workers G320b* on InfoSpace.

Appendix 2 – Data processing register

This should include:

- the purposes for which the data is processed
- who the data is shared with
- a description of categories of data subjects and the categories of personal data, including if the data is **sensitive personal data**[5]the conditions for the lawful processing of sensitive personal data are substantially unchanged but the GDPR will mean that we to restrict processing to what is necessary, and this may further limit the processing of such data in practice.
- the categories of recipients of the data
- any transfer of data outside the EEA
- the anticipated periods of storage for the different categories of data
- the technical and organisational security measures used to safeguard the data · It is advised that this register also contains the legal basis for processing the data, including any legitimate interests relied upon, the processing activities associated with the data and the location of the data. This will help to identify subject rights associated with the data e.g. we will be able to respond more easily to data subject access requests within the time frame.

Appendix 3 – Examples of automated decision making

- Recruitment – including automated rejection or shortlisting
- Performance management/triggers for sickness absence
- Health
- Behaviour
- Location
- Employee monitoring

[5] Sensitive personal data is defined as 'genetic and biometric data as well as data regarding racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life and sexual orientation.

Appendix 4 – Table of changes

Date of change	Paragraphs affected	Summary of update
19/09/2019	All	Complete review of document in light of DPA 2018 and GDPR now being brought into force. Updated the Subject access paragraph to clarify: when day one of the 'one month to respond' requirement begins and when the one-month period ends and; made it clear that there are exemptions around references. Also renamed the document 'Data Protection Act 2018 and GDPR Guidance' from 'General Data Protection Regulations Guidance'

08/01/2018	Pg 2 introduction Para 2 Para 2 Para 5 Para 3	Updated in light of NCC's ICT Services 4 Education traded offer Made it clearer why consent should not be relied upon Made it clear that legitimate interests as a legal basis for processing cannot really be used within public authorities (our basis for processing is in the public interest) Added a section detailing what individuals rights are and when they apply Added links to example gov.uk privacy notices for schools to issue to staff (and parents and pupils) Added link to new ICO GDPR guidance Changed the layout so that consent, privacy notices and special categories of data are sections in their own right
	Para 17 See contents for relevant sections.	
06/10/2017	Pg 2, 3, 5, para 2.1	Updated to: · give a better definition of personal data (pg 2 footnote) · make it clear that GDPR applies to electronic and structured paper filing systems (guidance given on how to define what is structured) pg 3 · make it clear that only schools and academies with over 250 employees must keep a data risk register. Schools and academies with under 250 employees only must keep one for high risk data only (ie high risk processing and processing of special categories of personal data (what was sensitive personal data) para 1 pg 5 · updated 'sensitive personal data heading to be called special categories of personal data para 2.1

29/08/2017	1,2,3,7,10,11,15	Paragraphs updated to provide more detail about what the section means in practice. Para 15 is a new para detailing information about the Data Protection Officer requirement.
10/08/17	All	New document to provide an overview and advice on how to prepare.