GDPR - QUESTIONS / QUERIES

1. What is GDPR?
   The General Data Protection Regulation (GDPR) comes into force on 25 May 2018 and replaces the current Data Protection Act 1998 (DPA).

   Under the Data Protection Act, organisations were thought to be compliant until there was a data breach. Under the GDPR, this is no longer the case, you need to have evidence that you are compliant from the start. This means that you need to have documents and processes in place to demonstrate you are following the regulations and ensuring the safeguarding of the data that you hold.

2. When does it come into effect?
   GDPR comes into force on 25th May this year.

3. Who does the GDPR affect?
   Any organisation that holds, collects or uses customer data for their business communications or marketing. Whilst there are legal changes under GDPR, if you have rigorous policies and processes in place currently under the Data Protection Act, then you are in a good position already, and should find it relatively straightforward to plan for, and demonstrate, GDPR compliance.

4. What do we need to do?
   You will need to review your processes and ensure they are compliant by the deadline.

5. What are the penalties for non-compliance?
   Organisations can be fined up to 4% of annual global turnover for breaching GDPR or £20 Million. This is the maximum fine that can be imposed for the most serious infringements e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach, or not conducting impact assessments. It is important to note that these rules apply to both controllers and processors meaning that 'clouds' will not be exempt from GDPR enforcement.

6. Will privacy notices need to be altered, relating to Free Early Education?
   KCC is reviewing and updating information relating to the General Data Protection Regulations.

7. Will KCC parental declarations need to be altered, from 25th May? (they may be considered not relevant & excessive for all age ranges)
   Yes, the GDPR requires that all information provided to people about how you process their personal data must be "concise, transparent, intelligible and easily accessible". It must be written in clear and plain language.

8. Will KCC need to update their retention of records toolkit?
   KCC will be reviewing our information and will update as required. Providers should also update their own policies.

9. Will providers need to review storage & disposal of records?
   Yes, this is required under the current Data Protection Act. It is important to have a clear and detailed understanding of what information you hold, what it is used for, how it is stored, and who it is shared with. You should consider both software systems and paper files. The Information Commissioner's Office (ICO) has produced a range of information which is available on their website. This mapping will help you identify any particular risks that need further follow-up and will help you identify any risks.

10. Will providers need to review their registration / admission paperwork and consent for photos websites etc?
    Yes, each document type needs to be assessed separately. In the case of many types of document, it will be sufficient to keep them only for the period required by statute; others will be essential reference material in future years and the organisation might, therefore, decide to keep them longer. Where consent is required, e.g. around taking and use of photos and videos of children, consent statements should be very clear, and multiple issues requiring consent should not be bundled into one consent statement.

11. If a setting was to close, they are required to retain records, but do they need to retain their membership of the ICO?
    Query raised with the ICO

12. Will providers need to review how information is transported (locked bags, cars etc)?
    Yes, this is also required under the current Data Protection Act.

13. Will providers need to ensure that Ofsted are aware of files being kept offsite?
    Yes, this is also required under the current Data Protection Act and also to make sure information is kept secure.

14. Will KCC need to inform providers how they store and email data to and from them?
    KCC is currently reviewing our policy and all its privacy notices and these will be accessible on KELSI and Kent.gov.uk.

15. Will providers need to update their staff contracts to ensure permission is gained to use photographs and any personal information in the setting, advertising and website?
    Yes, this will need to form part of your HR review.

16. Please clarify to providers when recruiting staff on retaining paperwork relating to the recruitment process. Queries raised relating to 'CVs on file'.
    It is the responsibility of any employer to set retention periods that are based on a clear business need. You must ensure that no recruitment record is held beyond the statutory period in which a claim arising from the recruitment process may be brought unless there is a clear business reason for exceeding this period.

17. Where is KCC 'cloud' located?
    The KCC cloud is secure.

18. Please clarify regarding the parents' 'right to erasure' i.e. can a parent request this when they leave/take their child out of the setting?

    As a childcare provider, you are required to process certain data. Things like accident records, for example, are a legal requirement and need to be kept for a set number of years. GDPR does not override this so you still need to comply with these data retention periods. The GDPR does not change the data that you need to collect, or how long you keep it for. If there is any data that you are keeping that does not NEED to be kept, then you should think about deleting it. The less data you hold, the less risk there is of a data breach.

19. Will databases/lists with for example, a collaboration lead name on, owner and manager information, such as addresses, personal emails etc all need to be reviewed?
    Yes, KCC will be reviewing this and will be notifying providers in due course.

20. Should providers be displaying allergy information in main areas?
    This information (or any personal information) should not be displayed in main areas or be easily accessible, however care needs to be taken to ensure staff are aware of a child's particular allergy.

21. How do providers having emergency contact details relating to the collection of children know that the emergency contact has given permission?
    You will need to have spoken and agreed this with the parent or carer. You will need to inform parents that you are making changes to your processes and consent arrangements so that you are compliant with the GDPR.

22. Will we need to ask for specific permission to send information and marketing promotions to providers via email (e.g. bulletin, training offers, etc.) – hopefully this issue has already been identified because it will require obtaining permission from each provider (unless the email address we use is already in the public domain i.e. preschool business email address)
    Yes, this needs to form part of your review and included in your privacy statements and opt-in processes. Withdrawing consent needs to be made easy to do.

23. Should providers be using personal emails instead of business ones as per (mentioned in the Kent Provider Agreement)
    Providers need to review the security they have around their emails. ***Personal email addresses should not be used.***

24. Where can I get more information?
    Providers can refer to:

https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf