Data Protection and Security Policy

Data protection statement
LKMco is registered with the ICO (Registration number: 00043243019) and at all times LKMco follows and complies with the 'data protection principles' set out in the Act, ensuring that all personal information collected is:

1. used fairly and lawfully
2. used for limited, specifically stated purposes
3. used in a way that is adequate, relevant and not excessive
4. accurate and up to date
5. kept for no longer than is absolutely necessary
6. handled according to people's data protection rights
7. kept safe and secure
8. Not outside the European Economic Area unless that country or territory ensures an adequate level of protection.

Our Data protection policy:

- *ensures that a nominated officer is responsible for data protection compliance and provides a point of contact for all data protection issues*
- *establishes appropriate retention periods for personal data*
- *ensures data subjects' rights can be appropriately exercised and that queries about data protection, internal and external to the organisation, are dealt with effectively and promptly*
- *provides adequate security measures to protect personal data and sets out procedures for sharing*
- *ensures that all staff are made aware of good practice in data protection and that there is adequate training for all staff responsible for personal data*
- *ensures that everyone handling personal data knows where to find further guidance*

Nominated officer
Dr Sam Baars, Director of research is LKMco's nominated officer for data protection and any queries about data protection procedures should be directed to him.

Retention and storage of data
In order to further LKMco's objectives of using evidence and data to inform education and youth policy and practice, LKMco collects and stores data and where subjects give permission, retains this data for an unspecified period, as long as LKMco deems the data to be of potential use in research. Data are reviewed every 5 years after their collection in order to judge whether or not they continue to be of potential use. Alternatively, subjects may request that we destroy their data at any time. Where subjects give permission, anonymised data may also be deposited in a data archive in order to allow other researchers to access and use it. We pursue this policy because in many cases, the power of data comes from its longitudinal or historic nature, as well as the opportunity to link together data sets. However, in some cases a shorter retention period will be explicitly set out. This is particularly likely to be the case where data is of a sensitive nature. Data will always be stored securely in encrypted form and where practical, it will be kept in anonymised form. Records of any personal data will be kept up to date in the 'personal data audit' spreadsheet (in google docs) and include a 5-yearly review date to judge whether the data remain of potential research use (and should therefore be securely retained) or should be destroyed.

Data will be transferred and removed from online survey platforms and dictaphones as soon as possible (for example, survey data may be gathered using the password protected 'survey gizmo' platform but will be saved in encrypted form as soon as the survey closes and deleted from the platform). Audio of interviews should be submitted using Typeout's secure system with "Please deliver to (name's) dropbox folder" (ensure they have your sookasa 'files delivered to' address - Login to the sookasa webpage, click on 'file delivery' and copy the link.)

Where physical records of personal data are kept these will be kept in a locked cabinet, however wherever possible, physical copies will be shredded and electronic copies only kept in encrypted form.

Data subjects rights and data/access queries
Where possible queries or requests for access from data subjects will be dealt with within a week by the member of staff initially contacted. Where further guidance is needed queries will be passed on to the Data Controller (Dr Sam Baars) or the Director, (Loic Menzies). If a period of more than a week is needed, subjects will be informed as to the reason for the delay and given an estimated period within which their query will be answered.

All consent forms inform participants who to contact if they have any queries about their data.
Where consent forms are not used - for example where data is gathered online, privacy notices will be included where:

- The information collected is sensitive
- The intended use of the information is likely to be unexpected or objectionable; or
- Providing personal information, or failing to do so will have a significant effect on the individual; or
- The information will be shared with another organisation in a way that wouldn't be expected

Privacy notices will comply with guidance provided by the ICO. They will also state that data will be stored and processed and their rights protected in line with the data protection act.

Staff education and training
All staff will undertake data protection training on an annual basis.
Data protection procedures, guidelines and training are reviewed annually in July.

Outsourcing and sharing
Where personal data is processed by, gathered or analysed by organisations external to LKMco, these organisations this will need to be done in an encrypted form and organisations will need to provide sufficient guarantees about how they will protect the data for the purposes of the data in question.

Beyond outsourcing, data will only be shared with other external organisations in non-attributable, anonymised form or where LKMco is legally obliged to do so.
.

Data and IT security

LKMco operates a well-managed ICT infrastructure and we have sought, and will continue to seek, independent expert advice to ensure compliance with the required standards.

- We ensure LKMco adheres to HM Government Cyber Essentials criteria

- We will not transfer personal data out of the European Economic Area, countries which are granted to have Adequate Levels of Protection as defined by the European Commission, or where transferred the US, such services will have adopted 'model clauses', for example Google Apps.
- We will review our systems and infrastructure annually in July.
- LKMco employees and subcontractors will only use computers and hardware approved for the task in hand
- We will use and maintain an audited, individual and organisation wide, secure password repository, such as 1Password. All passwords will be strong and where possible, unique to each login. Passwords will not be stored in browsers
- Strong passwords will comprise at least eight characters; differ from the associated username; contain no more than two identical characters in a row; will not be a dictionary word, date of birth etc; will include a mixture of numeric and alpha characters; have not been reused within a 6 months.
- We will use, where available, 2-factor authentication for all logins
- Role based logins will be used across all computer hardware and software, and only the appropriate level of permissions given to each user Our computers will have an up-to-date, industry standard virus scanner active and installed, and computers will be scanned on a daily basis or in real-time, where possible
- Our computers will have an up-to-date, industry standard firewall active and installed
- All users will access LKMco email via Google Apps, using strong passwords and 2-factor authentication
- All laptops, storage media and backups will be encrypted to at least FIPS140-2 or equivalent standard
- Where we store personal data in the cloud, for example in dropbox or google docs, it will be stored using our encrypted, and password protected, Sookasa cloud storage platform
- When working with personal data, we will ensure the screens of computers are locked if left unattended

With reference to the data used for any Department for Education project LKMco will:

- Provide a written description of the technical and organisational methods employed by the Contractor for processing Personal Data, if required
- Segregate DfE from non-DfE data on LKMco computers, and when in the cloud DfE data will be stored in a separate area of our encrypted, and password protected, Sookasa cloud storage
- Within an agreed timeframe after the project delete all personal data will and securely dispose of hard copies through shredding
- Keep hard copies of all documents in locked filing cabinets and never leave them out on a desk
- Hold secure back-ups of the DfE data we hold and shall ensure that up-to-date back-ups are stored off-site
- Keep an audit trail of where the DfE data is held, including software, cloud, hardware, laptops, drives and devices