GDPR Guidelines for staff - for reading and signing

The General Data Protection Regulation (GDPR) is a piece of EU-wide legislation which determines how people's personal data is processed and kept safe, and the legal rights individuals have in relation to their own data.

'Personal data' means information that can identify a living individual.

The regulation applies to all schools from **25 May 2018**, and will apply even after the UK leaves the EU.

Main principles

The GDPR sets out the **key principles** that all personal data must be processed in line with

- **Data must be:** processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected

There are also **stronger rights for individuals** regarding their own data.

- **The individuals have a right to:** be informed about how their data is used; have access to their data, rectify incorrect information; have their data erased; restrict how their data is used; move their data from one organisation to another; to object to their data being used at all. Please read the Trust's Privacy Notices for staff and parents

How this affects you, your school and the Trust - please read through this guidance carefully

Processing and Using Data

- The Trust must appoint a Data Protection Officer (DPO) and a Data Controller, who will advise on compliance with the GDPR and other relevant data protection law. Our DPO is Rebecca Leek. She is contactable at rebecca.leek@asseteducation.co.uk. The Trust Data Controller is Dale Collins. He is contactable at dale.collins@asseteducation.co.uk Any queries on data protection should be directed to both of these people. The headteacher in each school is the representative of the Data Controller on a day to day basis.
- The Trust has provided privacy notices for Staff, Parents and Pupils to demonstrate how we use personal data. You should make yourself familiar with these notices.
- If you receive a request from a parent about the data held by the school this is called a "Subject Access Request". All requests should be passed immediately to the headteacher who will discuss with the DPO. Schools will only have a month to comply with these requests so no time can be wasted.
- Most data held by a school is held on the lawful basis of fulfilling a public task. This includes class lists, assessment data etc. It is essential that this data is held securely and kept confidentially. It should only be shared with people on a 'need to know' basis and you need to consider where copies of data have gone. For example, you might well share a class list with a volunteer parent reader but would ensure that they didn't take the list home with them. Printed copies of class lists should not be provided for parents as Christmas or birthday invitation lists to take home from school. In the course of your work as a member of staff you might keep confidential data ie class lists, dates of birth, assessment notes in files in your classroom, or on your laptop or school computer, or on google drive.
- In order to carry out their role in 'supporting and challenging' the school, Governors do not need to have access to individual pupil information or special category data that identifies an individual.
- For some members of staff, during the course of your role, you may have access to, or are required to process, "special category data" eg information about racial or ethnic origin, religion, health, safeguarding, SEND or free school meals. If there is a data breach involving special category data then this can cause increased levels of distress for the person whom it concerns. This data should have additional safeguards to protect it and you should have a high level of awareness if you need to use this data as part of your role. You should consider the "need to know basis" and only share internally without additional permissions. In most

cases we will be sharing data on a lawful basis as it is in the vital interests of a child or we are performing a task in the public interest. This data sharing must continue eg safeguarding referrals.

- It is essential that any new sharing of data externally is reported to and reviewed by the Data Controller and the Data Protection Officer before this sharing commences.
- There are a number of activities that we do as part of our normal business for which we now need to obtain consent from parents. We can no longer send blanket marketing emails or texts without consent. We can, however, send an email out to a group of parents that directly refers to their child's learning or activities in school eg a reminder to bring wellies, etc. There is a consent form that parents will be asked to sign relating to the most common activity and data sharing in schools. Where the school needs an individual's consent to process data, this consent must be freely given, specific, informed and unambiguous. The consents will need to be recorded on Scholarpack.
- Any new personal data sharing that you wish to implement (this includes new pieces of software, external research projects etc) will need to be discussed with the Data Controller and the Data Protection Officer. The Data Protection officer in liaison with the Data controller will decide on the lawful basis for the data sharing to ensure GDPR compliance. If we decide that consent is required, then it will need to be obtained before the data sharing can commence. A Data Protection Impact Assessment (DPIA) may also need to be completed. Please contact Dale and Rebecca at the earliest opportunity for advice on what will need to be completed.
- We now need to obtain parental consent in order to be able to use some pieces of software where pupil information is shared with third parties ie Tapestry.
- In order to be able to use and share a child's photograph or piece of film beyond the school we need to obtain parental consent. You will need to check that this has been received. Named photographs of children should not be shared publicly eg on social media, school websites, brochures, etc, without an additional consent form which should be stored in a pupil's file.
- Parents may withdraw consent at any time so you need to be aware that this could happen and make the necessary arrangements.

Securing data - keeping data safe and securing your devices

- All staff laptops and devices owned by the school will need to be encrypted in order to be taken offsite. Ensure that personal data kept on your computer is kept to a minimum and that your laptop is always held securely. Uploading documents to google drive is recommended. It is not expected that USB sticks will be used. Please note: a small number of staff require the use of USB sticks as a part of their role including technical staff. It is the responsibility of the owner to ensure that these USB sticks are encrypted or that no personal data is stored on these. Also some older laptops will require USB sticks to enable them to turn on - these should only be used for this purpose.
- All personal devices used for work that store or use personal data will need to adhere to the same standards as school owned devices. This involves encrypting your device, most commonly by setting a pin/password on your device. If you are unsure or would like further advice on this please contact your IT Technician.
- Schools should make sure that personal information about a child, including medical and dietary requirements, should not be displayed in places where the information will be seen by a wider range of people than need to view it, including visitors. So think about where you display this information carefully and whether staff room notice-boards are appropriate.
- Information about individual pupils should not be left on desks and should be kept out of view ie in a drawer or cupboard. If you are using "special category data" please ensure that additional measures are in place to protect this. e.g locked cupboards/rooms etc.
- Google is a GDPR Compliant environment as long as your password is strong and not shared with anyone else. However, personal data that identifies individuals should not be sent by email unless the document is password protected or it is sent by encrypted email. Any google docs containing personal data should not be shared beyond the trust and should be kept on a 'need to know basis' within the trust. Where possible data should be anonymised.

Breaches of Data

- It is essential that we now record and investigate every data breach, however small. An analogy here might be the 'accident log book'. Whilst a child grazing a knee may be minor in isolation, if each incident is reported and a trend around a piece of playground equipment is spotted, some remedial action might be appropriate. And, so it is with data protection: if a particular system or process is identified as regularly having minor incidents by the Data Protection Officer, they and the school can mitigate the risk. They can only do this if a 'report it always' culture exists and is encouraged. It is imperative that you let the Data Protection Officer and Data Controller aware of any data breach however minor. **If you lose a laptop, mobile phone or other device containing school data this must be reported urgently.** The Data Protection Officer will decide whether to report the breach to the ICO. The Data Protection Officer needs to report this within 72 hours to the ICO should this be required so time is of the essence.

All members of staff within ASSET Education must read this guidance alongside the Policy and sign to confirm that they understand and will comply with it. Signed copies of this two page document need to be returned to the school office and kept in personnel files.

Signed _____ Name _____ Date _____