



Cheshire Academies Trust
Collaboration and Creativity

STAFF GDPR GUIDANCE



Next review date: Summer 2021

The General Data Protection Regulation (GDPR) came into effect on 25th May 2018 and it is essential that staff comply with the legislation as failure to do so may result in fines of up to €20 million.

GDPR relates to the personal data we collect as an organisation and how we process that data. Under the GDPR 'personal data' is described as information that relates to an identifiable, living individual, including information such as an online identifier, such as an IP address

Staff have an individual responsibility to ensure that they fully comply with the Trust policies in relation to GDPR. This means:

1. Always have GDPR at the forefront of your mind – in a similar way to safeguarding - when you use any personal data (staff, employees, governors, trustees, visitors), consider who is having access, why and whether appropriate authority exists to allow you to do what you are doing or whether you need to take additional steps.
2. Under GDPR, 'personal data' means any information relating to any person that is identifiable. This includes names on registers, lesson plans or exercise books, pictures and names displayed in or on the academy building and photographs on social media.
3. You should only access data if you have a legitimate business reason for doing so.
4. Data should only be shared externally if we have permission to do so from the data subject or we are required to share it via law or contract. More details regarding the types of information we collect and share can be found in the Trust's Privacy Notices on academy or the Trust's website.
5. Data being shared externally should only be done so via secure email account. The people in your academy with a secure email account are the Principal, the Vice-Principal, the SENDCo and the academy office staff.
6. Keep your laptop / computer locked when you are not in front of it and ensure it is password protected.
7. Personal data should only be accessed on Trust provided IT equipment. If you have not been provided with the appropriate equipment you require to fulfil your role please speak with your Principal in the first instance,
8. Personal ICT equipment such as mobile phones or other handheld devices should not be used to take / store photographs of children or data and should not be used to access academy / Trust email accounts
9. You should limit the amount of personal data you remove from your academy premises. If you need to do so, you must to take steps to ensure that it is secure:
 - Only use Office 365 for accessing personal data
 - Only use Trust provided equipment for accessing personal data;
 - Ensure your work laptop has a secure password and is not used by anyone else;
 - Only use your academy provided email address for school business;

10. Be aware that people have a right to see anything that is recorded about them. This includes emails, notebook or diary entries, text messages etc. Any personal information you record must be factual and necessary.
11. Do not print personal data unless absolutely necessary. Any data printed, should be kept securely and destroyed as soon as possible or in line with the Trust's retention schedule.
12. Keep your desk clear of all personal data items such as pupil or staff information.
13. GDPR requires our Trust to report all data breaches within 72 hours (regardless of weekends or school holidays). If you become aware of any breach of GDPR, you must advise your academy Principal without delay
14. GDPR allows any person (or parent if on behalf of a child) to request a copy of the personal data we hold on them via what is known as a Subject Access Request (SAR). As an employee of the Trust you may find yourself in receipt of a SAR via post, email or message. Under GDRP the Trust must respond to all SAR's within 30 calendar days. If you receive any communication which you think may be an SAR you must inform your Academy Principal without delay.
15. Each academy in Cheshire Academies Trust has an appointed GDPR Lead and GDPR Governor. If you are unsure about whether a matter is GDPR compliant or have any questions relating to GDPR please contact your GDPR Lead who will advise.
16. GDPR requires our Trust to appoint a Data Protection Officer (DPO). In CAT the appointed DPO is Luci Jones, CAT Director of Operations.