In the way I understand the scenario the employee is being asked to take the information home with a company file. I do not believe that it would be appropriate to just take a file home that is not secure and that contains personal data and information. There are both state and federal laws in place that protect personal information across all industries although some of the details are subject to state laws more specifically.

The very act of taking a file home isn’t necessarily unacceptable but it should definitely be treated with complete legal regards or you are taking a risk that in my opinion is not worth the risk. The file shouldn’t be transferred or copied onto a personal computer in any way. The best way to deal with this would be to use a company laptop that is appropriately secure or to be able to remotely login to a secure network to access the file and data that pertains to the employees. This would ensure a close and secure network and not put yourself in any risk of doing something with personal data that you were not even aware of in the first place.

If the file then only contained information of personal names and departments, I believe that this information would be ok to transfer and to take home to work on a personal computer. Names and departments do not seem to be included in private information. With that said, I would still probably not do it. I would, if at all possible, still try to secure the file in some way in order to protect the information for best practice.

Resources:

<https://www.itgovernance.eu/blog/en/the-gdpr-what-is-sensitive-personal-data>

<https://www.cio.com/article/3156565/should-software-developers-have-a-code-of-ethics.html>

<https://www.asha.org/practice/ethics/confidentiality/>.