

## Informationen zum datenschutzgerechtem Umgang mit E-Mails:

- **E-Mails versenden:** cc: versus bcc: Datenschutz bei mehreren Empfängern
  - Wer ein- und dieselbe Mail an einen größeren Adressatenkreis verschicken will, muss sich genau überlegen, wie er das tut. Wenn jeder Adressat sehen kann, wer die Mail noch erhalten hat, liegt im Regelfall ein Verstoß gegen den Datenschutz vor. Die Devise bei Adresslisten muss deshalb lauten: Versand per „bcc:“ statt „cc:“!
  - Wer alle Empfänger einer E-Mail in das „An:“- oder das „cc:“-Feld der E-Mail schreibt, liefert den Empfängern nicht nur die Information, wer alles diese Mail empfangen hat, sondern auch gleich noch die dazugehörigen E-Mail-Adressen - mit anderen Worten also schützenswerte personenbezogene Daten.
  - Oft wird übersehen, dass es nachhaltige Probleme der Datensicherheit nach sich zieht, wenn Mails in der beschriebenen Art und Weise verschickt werden. Dazu weist die hessische Datenschutzaufsicht auf Folgendes hin:
    - Einige Schadprogramme verschicken sich selbständig an jede E-Mail-Adresse, die sie auf dem befallenen PC finden. Sie können Funktionen beeinträchtigen, vertrauliche Daten ausspionieren oder Spam versenden. Wird das oben empfohlene Verfahren (Versand über „bcc:“) angewendet, können höchstens zwei E-Mail-Adressen betroffen sein. Ganz anders sieht dies im Fall einer Massen-E-Mail mit offenem Adressatenkreis aus.
    - Hinzu kommt, dass durch die Versendung mittels einer offen gelegten Adressliste die erhaltenen E-Mail-Adressen von den Empfängern für unverlangte Werbe-E-Mails genutzt werden können („Spamming“).
    - Haftungsrechtliche Konsequenzen können die Folge sein.
- **E-Mails beantworten:** „Antworten“ versus „Allen antworten“
  - Sparsamer Umgang mit der Funktion „Allen antworten“.
- **E-Mails „Weiterleiten“**
  - Auch E-Mails unterliegen – wie Briefe – einer gewissen Vertraulichkeit. Man sollte daher E-Mails nur dann weiterleiten, wenn man auch die Genehmigung des Absenders hat oder davon ausgehen kann, dass dieser mit einer Weiterleitung einverstanden ist.
- **Vertrauliche E-Mails** sollte man **verschlüsseln**, um den Inhalt möglichst sicher zu übermitteln. Mit einem E-Mail-Zertifikat im E-Mail-Programm können E-Mails und Dateien einfach und kostenlos ver- und entschlüsselt, sowie ihre Integrität (Unverändertheit) und Authentizität (Herkunft) mittels digitaler Signaturen abgesichert und überprüft werden.

Weitere Hinweise zum Datenschutz im Schulalltag unter <https://datenschutz.hessen.de/>

### Quellen:

- THM – Technische Hochschule Mittelhessen. Arbeitshilfe Datenschutz Nr.1. Datenschutzgerechter Umgang mit E-Mails.
- <https://datenschutz.hessen.de/>