Education Matters

GDPR, Data Protection and Data Cleansing

Date: Wednesday 13 March 2019

Brachers With you all the way

KRESTON REEVES

Session summary

The forum, hosted by Brachers and Kreston Reeves, focuses on topical issues and challenges that the education sector is facing.

This event was focused specifically on GDPR, Data Protection and Data Cleansing.

Data breaches

- Ensure staff are aware of what a personal data breach is and the action they should take following a breach.
- You must report a notifiable breach to the ICO without undue delay and no later than 72 hours of becoming aware of it.
- Not all breaches have to be reported. When considering if a breach should be reported assess the likelihood and severity of the risk to the individual's rights and freedoms, following the breach. If it is likely there is a risk you must notify the ICO. If a breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform the individual(s) without delay.
- Ensure that you have robust breach detection, investigation and internal reporting procedures in place. This may be set out in your data-protection policy or a separate policy. It is important to ensure that staff are trained and made aware of these procedures.
- When reporting a breach to the ICO, you must provide certain specific information. This includes a description of the measures taken, or proposed to be taken, to deal with the breach, including any measures to mitigate any possible adverse effects.

Subject access requests

- You must act on a subject access request without undue delay and at the latest within one month of receipt.
- You can extend the time to respond by a further two months if the request is complex, or you have received a number of requests from the individual. There is little guidance on what will be 'complex' but the ICO have given us some indication that it is likely to apply in very few circumstances and generally you will be expected to have systems in place to comply with the initial one month time limit.
- Know what personal information you are collecting and processing, where information is kept, where and by who, as this will make acting upon a subject access request within the required time limits much easier. Carrying out a data mapping process may assist with this.
- Ensure there is a policy in place which sets out how requests should be acted upon and by who and that all staff are aware of this.
- When receiving a request from a parent consider whether the student is competent enough to make the request themselves. If so, you may need to refuse the request unless made directly by the pupil.
- If Governors are using a personal email address, ensure that they are aware that if a request is received, a review may need to be undertaken of their emails.

Know your policies well but remember to always consider the facts of each scenario and take relevant advice where necessary.

Continued on next page...

Brachers With you all the way

www.brachers.co.uk
01622 690691

Head Office
Somerfield House
59 London Road
Maidstone
Kent ME16 8JH

@brachersllp

Brachers LLP

Education Matters

GDPR, Data Protection and Data Cleansing

Data retention

- Ensure that you have a data retention policy which can be realistically followed and actually is being followed.
- Conduct regular reviews and delete any data for which retention is not necessary.
- Regularly reviewing and deleting data will make complying with subject access requests much easier
- Consider whether paper documents can be scanned and destroyed. Electronic storage can be more secure.
- Delete all historical data which has been kept for a time beyond any of the limits set out in your data retention policy.
- Consider collecting in paperwork that contains personal information at the end of governors meetings and that this is retained in one place at school or, if possible, destroyed as opposed to being kept at the home of the Governor, possibly unsecured.

Cyber security

- Ensure staff and students are aware of the importance of cyber security and how they can prevent cyber-attacks.
- If you have a 'bring your own device' to work policy or staff work remotely then ensure they are aware of the need to be cyber aware while using their own devices.
- Provide training to staff so that they understand acceptable practice in your organisation, for example, emails from unknown senders and/or clicking on attachments should not be done.
- Ensure staff and/or students are aware of the social media policy that your school has in place and know what they can and cannot post in relation to the school and its students.
- Make clear that strong passwords and encryption software should be used where possible and regularly reviewed and updated.

Key points

1. Identify all of the personal data that you hold and where it is held.
2. Regularly review privacy notices and ensure they are compliant with legislation. Also consider if there should be a separate privacy notice for children?
3. Establish a policy for handling data breaches, ensure this is communicated and staff are trained in this.
4. Provide regular staff training on data protection responsibilities.
5. Develop and implement a policy on retention and storage of data.

Key contacts

For further advice regarding any of the topics discussed please contact us.

- Louise Brenlund
  louisebrenlund@brachers.co.uk
  01622 776405
- Phil Reynolds
  phil.reynolds@krestonreeves.com
  0330 1241 399

All content correct at the time of print March 2019.