One Education Staff - GDPR Acceptable Use of Personal Data Policy

1. Statement of responsibilities

Individual users are responsible for their own actions.

Every user of One Education Ltd information technology systems has a duty to ensure they practice appropriate and proper use of personal data and must understand their responsibilities in this regard.

For One Education Ltd to be as effective as it can be when it comes to GDPR compliance and standards, it is important that all staff understand the standards of practice which they are required to adhere to when processing any personal data whilst carrying out their role for One Education Ltd.

Under no circumstances should emails from One Education Ltd systems, (other than those relating directly to the staff member for example pay slips and HR documents) be forwarded to personal email addresses.

If staff have any questions or queries relating to GDPR or what this all means for them from an operational point of view, guidance and advice can be found from any of the following locations;
Telephone: 0844 967 1111
Email: dpo@oneeducation.co.uk Our policies are available here: https://www.oneeducation.co.uk/about-us/our-policies/

Staff are also referred to One Education Ltd Data Protection Policy for detailed guidance.

A failure to comply with internal GDPR Guidance, Policies and/or Procedures may result in disciplinary action being taken.

2. Guidelines for acceptable use of email

Composing e-mails

- Emails are a form of corporate communication and therefore should be drafted with the same care as letters.
- Email is disclosable under the Freedom of Information and Data Protection Regimes. Be aware that anything you write in an email could potentially be made public.
- Keep emails brief.
- Never put personal information (such as a employee/pupil name) in the subject line of an e-mail.
- Limit recipients to the people who really need to receive the e-mail. Avoid the use of group address lists unless it is absolutely necessary.

- When sending emails containing personal or sensitive data always respond to an authorised, approved address.
- If possible, try to stick to one subject for the content of each e-mail, as it will be easier to categorise it later if you need to keep the e-mail.
- Understand how to use CC and BCC in e-mails. (See appendix for details)
- Check the recipient's name, especially if there is more than one person with the same name.
- Be careful when replying to emails previously sent to a group. Choose "Reply" rather than "Reply all".
- Change your email settings to default 'Reply' and not 'Reply only' in email settings. You can do this by using the cog on the right, choosing mail options at the end of the menu then choosing email and reply settings.
- Before sending an e-mail, always check the recipient's email address to make sure it's correct.
- One Education Ltd "predictive text" system is designed to assist but be extremely careful when considering options. Ensure you only choose the correct and most up to date email address for the recipient.

Sending Attachments [This section to be updated in Summer Term following the roll-out of the Egress System]

- Avoid sending sensitive information in an email. Sending an email is like sending a postcard through the post. Confidential or sensitive information should only be sent by a secure encrypted e-mail system.
- Teams who deal with sensitive personal data should ensure that communications which are sent are either password protected or encrypted. If colleagues are unsure as to the appropriate level of protection required, they should seek specific guidance on what is expected from their line manager. Guidance on how to encrypt or password protect communications should be obtained from the ICT department in the first instance.

Filing e-mails

- E-mail systems are commonly used to store information which for security purposes should be stored elsewhere.
- Where the main purpose of the e-mail is to transfer documents, then the attached documents should be saved into the appropriate place in an electronic filing system or printed out and added to a paper file. The e-mail can then be deleted.
- You should file emails in line with your Team's current practice. If you are not clear on your Team's current practice, please check with your Line Manager to ensure you comply with One Education Ltd expectations.
- In the event you are sending an email with advice:
    - Pertinent to the progression of the case;
    - Setting out the legal pitfalls/advantages;
    - You suspect the school will not want to follow;
    - Following on from a phone call, you feel is important to set out in writing;
    - Has the potential to become litigious.

You should ensure it is saved in the relevant casework file in the M Drive (see below for instructions on how to do this)

Retention of Emails

- E-mail is primarily a communications tool.
- E-mail applications are not designed as a storage area.
- You should retain emails in line with your Team's current practice. If you are not clear on your Team's current practice, please check with your Line Manager to ensure you comply with One Education's expectations.

- In the event you are sending an email with advice:
    - Pertinent to the progression of the case;
    - Setting out the legal pitfalls/advantages;
    - You suspect the school will not want to follow;
    - Following on from a phone call, you feel is important to set out in writing;
    - Has the potential to become litigious.

  You should ensure it is saved in the relevant casework file in the M Drive.

- IT have advised us to use Google chrome when saving emails to M Drive by following the process set out below:

  Open up the email
  Click on the drop down arrow (next to reply)
  Select 'Open in a separate window' (should be the very last option on the list)
  Click on the 3 dots next to junk
  Select 'Print' from the drop down list
  In the print preview, next to destination click on 'Change...'
  Under Print Destinations select 'Save as PDF'
  Select Save and then navigate to the relevant folder/destination in M drive
  You should now be able to view the email as a PDF.

3. Guidelines for acceptable use of Information Technology

- Staff must use IT equipment responsibly and for professional purposes only (this includes the use of mobile phone, if applicable).
- Any personal data held on One Education Ltd networks must be accessed appropriately and stored securely.
- Staff must not disclose their passwords or record them anywhere they could be found.
- All logins must be conducted through the remote desktop.
- USB memory sticks are not permitted for the storing of personal data in any form. (USB sticks are subject to a high risk of being misplaced and, as such, the safety of information stored on them cannot be guaranteed).
- Staff must not use cloud storage for the retention of One Education work emails, documents or information related to the company and its business in any way unless the storage has been provided by One Education (i.e. through the

organisation's shared spaced on office 365 or One Drive). If you have concerns regarding the locations which are acceptable and compliant to store the information, please refer to the ICT team in the first instance.

- Ensure your computer screen is locked or logged out when not in use (this includes leaving your desk unattended when in the office).
- Do not store documents on your desk top or personal drives or use personal computers to undertake work.
- Only use Remote Access to access One Education Ltd files.
- Only use One Education Ltd approved electronic devices.
- Associates must always use remote access when working for One Education Limited.

4. Guidelines for acceptable use of paper based documents

- Paper copies of documents containing personal data may need to be retained. In such cases, the personal data must be stored safely in line with One Education's Data Retention Schedule.
- Once personal data (in paper format) has reached the end of its administrative life it should be safely disposed of in line with One Education Ltd Retention Schedule.

5. Guidelines for acceptable use of One Education Office Equipment

- Always log and log out of office printers/scanners correctly.
- Use confidential bins for destroying confidential documents.
- Address redaction in necessary circumstances when you do not need to share personal data.
- Always think about the most secure method of sending personal data.

6. Guidelines for keeping "data on the move" secure

- Minimise the amount of physical documentation you carry around when working off site.
- Use lockable bags where possible.
- Laptops, tablets and smartphones should never be left on a vehicle seat. Even when the driver is in the vehicle, their device could be vulnerable when stationary (for example, whilst parking or at traffic lights).
- Be careful about transporting documents from home to office, make sure any personal data is secure in your car. (If possible, store data in the boot of your car).
- Do not leave personal data in your car overnight.
- If working from home, ensure personal data is kept secure at all times.
- Ensure paper files are not left unattended at any time.
- Employees should keep mobile devices with them at all times. When unattended, they should be kept hidden or physically locked away.

7. Sending Physical Documents by post

If you want to send documents which contain personal data, you need to think about:

- What information you are sending and how sensitive it is
- Whether you are sharing personal data unnecessarily
- Whether you have done everything in your power to ensure the information gets to the right person.
- Whether sending by post is the correct way of transporting the personal data.

If you decide to send by post, you MUST:

Ensure the contact details are correct.

Ensure the Addressee is marked clearly with Private and Confidential marked clearly if relevant.

Ensure the information is securely sealed, ensuring the packaging is sufficient to protect the contents during transit.

Ensure a return address is included on the envelope in case it has to be returned for some reason.

When appropriate send the information by special delivery and charge the cost of the Special Delivery back to the client/school.

8. Guidelines for delivering physical documents by hand

It may be appropriate in some instances to personally deliver documents to a client/school.

If so, think about the process, to whom are you going to deliver to? The office/HT/Business Manager.

Think about the time spent delivering and ensure it is recorded. Check with the client/school in advance to agree the method.

If delivering direct to an employee's home. Think about the handover and ensure you feel comfortable.

Appendix – Use of CC v BCC

CC and BCC are both ways of sending copies of an email to additional people.

CC means carbon copy. CC is sometimes referred to as "courtesy copy," which better describes what a CC actually is. When you CC people on an email, the CC list is visible to all other recipients.

BCC means blind carbon copy. (In practice this means that no one but the sender can see the list of BCC recipients. A BCC recipient can see the email addresses on the

"to" and CC list together with the contents of the email but they will only be able to see their own email address on the BCC list.

CC is useful when:

- You want someone else to receive a copy of an email, but they aren't one of the primary recipients.
- You want the recipients of the message to know the other people who have been sent the message.

BCC is useful when:

- You want someone else to receive an email, but you don't want the primary recipients of the email to see you've sent this other person a copy. For example, if you're having a problem with a fellow employee, you might send them an email about it and BCC the human resources department. HR would receive a copy for their records, but your fellow employee wouldn't be aware of this.
- You want to send a copy of an email to a large number of people. For example, if you have a mailing list with a large number of people, you could include them in the BCC field. No one would be able to see anyone else's email address. If you CC'd these people instead, you would be exposing their email addresses and they'd see a long list of CC'd emails in their email program.
- You could even put your own email address in the To field and include every other address in the BCC field, hiding everyone's email address from each other.