GDPR

Frequently Asked Questions

Questions	Answers
Does GDPR mean that individuals now need to consent for us to hold their data?	No. Consent is one lawful basis for processing personal data but it is not the only one. Consent is not a silver bullet and should not be the default for processing personal data. In most cases data will be processed as part of a contract (such as the student or staff contract) or to meet a legal obligation.
Does GDPR mean that I need to get rid of all of my old files?	No. GDPR does not require us to dispose of all of our ‘old’ information. However, it does say that we should only hold personal information for as long as it was required for the purpose of collection. Therefore if there is a valid and reasonable reason to retain the information you are likely to be able to do so. However, if you no longer need the information then you should look to dispose of it.
Does GDPR mean that I need to get rid of all of my old emails?	No. As with other documents GDPR does not require us to dispose of all of our old emails. However it does say that we should only hold on to personal information in our inboxes for as long as it was required for the purpose of collection. Therefore if there is a valid and reasonable reason to retain the information you are likely to be able to do so. In general terms if you still have regular dealings with the individual then it is acceptable to retain the email. However, if you no longer need the information then you should look to delete the emails. Reviewing inboxes can be a large task for individuals therefore it can often be best to plan a thorough review over a number of weeks or months to make the task more manageable.
Does GDPR mean that I cannot display student’s work?	No. GDPR does not mean that you cannot display example of student’s work. However in order to comply with both GDPR and Copyright legislation you should seek the explicit consent of the student to display their work (or to anonymise it).
Does GDPR mean that I cannot keep exemplars of a student’s assessed work?	No. GDPR does not mean that you cannot keep good examples of student’s work to share with other students. However in order to comply with both GDPR and Copyright legislation you should seek the explicit consent of the student to display their work (or to anonymise it)
Does GDPR mean that I can’t display photos of individuals	No. Although, photos are personal data under GDPR however this does not mean that you cannot display them. The legislation is not specific on photographs however you should consider the individuals in the photographs and what the likely impact on them will be. Please see the College GDPR Staff Guidance document.

Does GDPR mean that I can no longer send information to the contacts on my database?	No. If you currently maintain a mailing list of contacts which you routinely send information out to it is likely that you can still continue use this. However, you will need to ensure that those individuals have given you their explicit consent to hold their information. You should contact them to ask if they are happy for you to hold their information and use it for **agreed and defined purposes**. If you do not receive a reply then you should remove their information.
Does GDPR mean that I can no longer display attendance register information on whiteboards for the entire class to see the information?	Yes. Information in the attendance register is personal information. However, you can use PCs which are available in all learning areas to display attendance registers but, make sure that you are not being overlooked by anyone when marking the register.
Does GDPR mean that I can no longer speak to parents and employers over the phone about learner issues?	No. GDPR does not mean that you cannot speak with parents and employers over the phone about learner related issues. However in order to comply with GDPR you must first check that we have received and logged onto Prosolution consent from the learner. The College will endeavour to collect consent from every learner at enrolment time.
Does GDPR mean that every breach needs reporting to the ICO?	Only breaches that lead to a risk to an individual's rights and freedoms need reporting to the ICO. When considering whether a breach needs reporting the College will need to think about the nature of the personal data involved; how easy is it to identify individuals; and what the consequences are of the data breach? The Data Protection Officer will decide on all cases of personal data breach whether to inform the ICO or not.

Other Specific Advice

• **Promonitor**	In regards to the use of promonitor and recording and sharing information, it essential that you consider where you are recording sensitive or personal information about a learner. The Comments section should only be used to share information that relates to educational impact, progress and attendance. Anything personal or sensitive should be logged in confidential information. For example A learner calls up to say that they will not be attending college because they have had a bereavement. • Note added to promonitor ' XXXX will not be attending college today (reason added to confidential'. • Confidential comment added detailing the bereavement A meeting is held to discuss why a learner is not attending. • Details of the actions required by the learner to improve attendance logged in the meeting slots on promonitor • Details of reasons why the learner has not been attending to be logged in confidential comments.

GDPR

Do’s and Don'ts

“GDPR requires a 180-degree turn in how organisations regard and treat personal data. We must get used to thinking about the lawful basis to process (viz. collect/access/use/store/send) that data, even if we have already collected it!”

1. When you process do ensure that it is accurate, relevant and not excessive in relation to your needs.
2. Do not process personal data unless you are sure that you, your team or the College have a lawful basis for doing so. In most cases the College processes personal data in performance of a contract with that person or to meet a legal obligation. In all other cases, do not process personal data unless you are sure that you, your team or the College has obtained the consent of the individual concerned.
3. Do not write any comment about any individual that is unfair or untrue and that you would not be able to defend if challenged. Remember anything that you write about a person will be seen by them should they make a subject access request (SAR).
4. If you download personal data from ProSolution or any other system to share internally or externally and save locally on a shared or personal drive it is considered best practice to mask that data. In particular, anonymise, pseudonymise or password protect it and when you no longer require it remember to permanently delete the file.
5. Do not disclose any information (including giving references) about an individual to an external organisation without first checking that the individual consents to such disclosure, or, in the case of the police, checking with the Data Protection Officer at dpo@accross.ac.uk.
6. Protect people’s privacy and personal data like it’s your own.
7. Do not project learner data, e.g. course register onto whiteboards, instead, use desktop computers provided in classrooms and other learning spaces for that purpose.
8. Only keep data for as long as is needed under our records retention schedule. If in doubt, please refer to the College Retention Policy.
9. Use a shredder or the confidential waste disposal bins to dispose of any document containing personal data, whether or not you consider it to be confidential.
10. Always lock your computer when you are away from your desk.
11. Ensure that all personal data is kept secure, not only from unauthorised access, but from fire and other hazards.

Apply password protection to computers, screensavers and documents. Where possible keep your office door locked and your desk clear of personal data when you are absent

Handling Personal Data offsite

Do’s and Don’ts

1. Avoid processing personal data offsite whenever possible.

2. Be vigilant if you are undertaking work off-campus using personal data such as individualised learner data, reference requests or examination scripts or results. Strict security measures must be applied to the transportation and storage of all such data E.g. password protection, encryption or secure managed file transfer.

3. Use the College’s central and secure shared I-drive to store and access personal data and sensitive information; this helps to ensure that only legitimate users have access to it.

4. Use the IT-authorised remote access facilities such as Virtual Desktop Infrastructure (VDI) that are both secure and encrypted to access personal data and sensitive information on the central servers instead of transporting it on mobile devices and portable media.

5. Do not use non IT-authorised third party Cloud services, like Dropbox or Google Drive when processing high risk personal data or sensitive information. The data might be held outside the EU.

6. If there is no option but to use mobile devices, portable media or email for high risk personal data or sensitive information, use encrypted devices or encrypt the data.

7. Do not use personal equipment, such as home PCs or personal USB sticks, to process high risk personal data or sensitive information

8. Always keep personal data and work related information separate.

9. Avoid sending high risk personal data or sensitive information by email or using email to store such information. If you must use email to send this sort of information, encrypt it. If you are sending unencrypted high risk personal data or sensitive information to another College email account, indicate in the email subject line that the email contains sensitive information so that the recipient can exercise caution about where and when they open it.

10. Do not process high risk personal data or sensitive information in public places. When accessing your email remotely, exercise caution to ensure that you do not download unencrypted high risk personal data or sensitive information to an insecure device.

11. Electronic keys for encryption, e.g. passwords, must be appropriately managed so that the College can always access the information.