The General Data Protection Regulation (GDPR)

STAFF GUIDANCE

Contents

1. Glossary

The following terms are used within the General Data Protection Policy (GDPR) and Guidance:

- **Personal Data** – information relating to an identifiable living person ('data subject')
- **Processing** – any operation or set of operations carried out on personal data including recording, organisation, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination, erasure or destruction.
- **Controller** – organisation, person or other body which alone or jointly with others, determines the purpose and means of processing of personal data.
- **Processor** – organisation, person or other body which processes personal data on behalf of the controller.
- **Third party** – organisation, person or other body, other than the data subject, controller or processor.
- **Consent** – of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- **Personal data breach** – beach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

2. Personal Data

The College and individual members of staff will have access to a wide range of personal data and sensitive information relating to learners, members of staff, parents, carers and employers.

Personal data is defined as any combination of data items that identifies a living individual (the data subject), who is identifiable from that information or who could be identified from that information combined with other data which the College either holds or is likely to obtain.

The data may be held in digital format or on paper records may include names, contact details, photographs, salary, attendance records, student marks, sickness absence, leave, dates of birth, marital status, personal email address, online identifiers, IP addresses etc. Furthermore any expression of opinion or any intentions regarding a person are also personal data.

GDPR covers all personal data processed by the College, irrespective of whether these data are held by individual members of staff in their own separate files held centrally on the College network or held outside College e.g. by staff working at home.

The GDPR also defines 'special categories of personal data' which relates to the following:

- The racial or ethnic origin of the data subject
- Their political opinions
- Their religious or philosophical beliefs
- Whether they are a member of a trade union
- Their physical or mental health or condition
- Their sex life or sexual orientation

'Special Categories of personal data' can only be processed under limited conditions. In the context of the College this would most often be:

- The individual has given their explicit consent
- There is a legal requirement to process this information such as immigration or equality requirements
- The processing is required for occupational health, absence management or the provision of health or social care services or treatment
- It is necessary for research of statistical purposes

Whilst not defined in GDPR, there are additional types of personal data which if disclosed could cause significant harm or distress. Examples of these include bank account details, national insurance number, copies of identity documents, date of birth etc.

3. Key considerations

Before embarking on any processing personal data, whether that be sharing personal data with a third party, using a new online tool, marketing a new programme or any other action that involves the use of personal data, you should ask yourself the following questions:

- Do we really need to record the information?
- Do we have a valid justification for processing the data i.e. it is required for a contract or has the data subject given their consent.
- Has the subject been told about the processing i.e. been issued with a privacy notice?
- Are we authorised to collect/store/process the personal data?
- Have we checked with the data subject that the personal data is accurate?
- Are we sure that the personal data will be secure during the process?
- Are there alternative ways the same objective can be achieved without using or sharing personal data?

If having considered the points above you conclude that the processing of personal information is necessary then the information in the following sections will provide more details about the factors that need to be considered and the actions that need to be taken to ensure the processing meets the requirements of GDPR.

4. Data Security

The level of security required should be assessed against the risks associated with the data being processed. Security should also be assured no matter where or by whom data is stored or processed and throughout the whole procedure, including the transmission of data. Appropriate measures must be taken to protect against unauthorised or unlawful access.

You should not process personal data out of college unless absolutely necessary. If it is necessary to process personal data out of college particular care should be taken to ensure the security of the data. Where information is being held or accessed on a mobile device it should be kept secure at all times with appropriate measures in place to prevent theft or interception of transmission. Where personal data is copied onto a mobile device, additional care is needed to avoid personal data becoming inaccurate over time.

All personal data stored on computer equipment or portable storage media must be deleted beyond retrieval
prior to equipment disposal.

Appropriate security measures such as encryption and strong password controls are considered further in the following College documents:

- Information Security Guidance

- Data Encryption Guide

5. Privacy Notices & Consent

When is Consent needed?

The GDPR requires that all processing of personal data has a lawful basis. Article 6 of GDPR gives a number of circumstances when processing personal information would be justified. Consent should be used when there is no other lawful basis for processing an individual's personal data. This may be the case if we want to use someone's data in a particularly unexpected or potentially intrusive way, or in a way that is incompatible with what we have already told them we will do with their personal data. For example, if we want to publish stories or images of individuals on the **website** or in publications we have to get their consent. Consent that has been obtained must be documented include details of what the individuals were told and when and how they consented. Individuals must be told that they have the right to withdraw their consent at any time and how to do this.

Under the 'fair and transparent' requirements of the first data protection principle, the College is required to provide data subjects with a Privacy Notice to let them know what we are doing with their personal data. The College has a number of Privacy Notices published on the College website www.accross.ac.uk. Two of the Privacy Notices relevant to this guidance for staff and students. These notices provide details to staff and students about what they can expect the College to do with their personal information. The notices also cover the various types of data processing that are **essential** to manage the relationship the College has with its staff and students and all that happens to their personal

data while it is held by the College. The majority of what the College does with personal data is necessary to the running of the College and is done in accordance with the contracts the College has with its staff and students.

If consent is being sought or a privacy notice being prepared in relation to a new activity which could have an impact on the privacy of the individuals concerned then consideration should be given to carrying out a Data Protection Impact Assessment (DPIA).

6. Subject Access Requests

All data subject has the right to obtain the following information:

- Confirmation that personal information about them is being processed
- A copy of that personal information
- Details of the purpose of the processing
- Categories of the personal data concerned e.g. does it include any special categories or sensitive personal information
- Any recipients or categories of recipients the personal information has been shared with, particularly if these are outside the EU.
- What safeguards are in place for transfers outside the EU
- The period the personal information will be stored for or what the criteria is for determining the period of storage.
- The existence of the right to request from the controller the correction or deletion of personal data or to restrict or object to the processing of personal data concerning them.
- The right to lodge a complaint with the Information Commissioner's Office
- What the source of the personal data is if it has not been collected directly from the data subject.

Any member of staff receiving a request from an individual for their own personal information should forward this to the Data Protection Officer as soon as possible (dpo@accross.ac.uk) for advice. The following points should help when dealing with a request.

- The request can be in **any format** provided it is clear.
- We should be satisfied about the **identity of the requester** before releasing any information. Proof of identity can be requested if required.
- If the **scope of the request** is not clear then we can asked the requester to be more specific about the activities and areas to which the request relates.
- Information must be provided in a **concise, transparent, intelligible** and easily accessible form using clear language.
- The response should be provided in a commonly used **electronic format**, particularly if the request came in electronically, unless the requester asked for another format. When requested by the data subject the information may be provided orally as long as we are confident about the identity of the data subject.
- Information should be provided within **one month**.
- Information must be provided **free of charge** unless additional copies are requested when a reasonable fee can be charged based on administrative costs.

7. Data Sharing

- **Internal Data Sharing**

It is part of the responsibility of the MIS Reporters to obtain information for teams and individual staff from the College main databases e.g. Prosolution, ProAchieve etc. Presently, datasets generated by the Reporters are usually sent to requestors by email. To enable the college to comply with GDPR, the following new internal data sharing process has been implemented.

- Reporting team receive email requesting information

- Reporting team generate requested dataset
- Reporting team store dataset on named I-Drive subfolder
- Reporting team restrict access to dataset in the named subfolder to requesting team/staff only
- Reporting team sends email the data requestor informing them that data is available for access in named subfolder.
- Requesting team / staff access dataset stored in subfolder

It is advisable that individual staff do not copy dataset from I-drive subfolder and store on local hard discs, USB pens etc.

- **External Data Sharing**

Before sharing any personal data with any outside organisation there are a number of things that need to be considered or questions that should be asked:

- Does the data sharing need to take place or could the objective be achieved in other ways?
- Are there any risks involved in sharing the personal data? If there could be, please contact the DPO on dpo@accross.ac.uk who will advise on how to conduct a **Data protection Impact Assessment**
- Does the sharing involve the transfer of data outside the EU?
- Which lawful condition of processing is being met?
- Have the data subjects been informed about the transfer via a Privacy Notice?
- Are all the data protection principles being adhered to?
- Is the third party acting as a processor for the College i.e. acting under the instruction of the College? If so there **must** be a contract between the College and the processor.
- Even if the third party is not acting as a data processor there should normally be a contract / data sharing agreement in place to ensure that the third party is meeting the legal requirements of GDPR.

If you are planning to set up a data sharing or data processing contract / agreement you should inform the Data Protection Officer: dpo@accross.ac.uk

8. Requests for Personal Information from Third Parties

The College tells students and staff how their information will be used, and in what circumstances and to whom it may be disclosed, through the relevant student and staff privacy notices, see http://www.accross.ac.uk/about-us/information-compliance/ .There are some third parties that can require disclosure of personal data, for example, parents, the police and the Department of Works and Pensions. Examples of how to handle certain common types of request are given in Appendix 1.

9. Transfer of Personal Data Outside the EU

For more advice on transfers of personal data outside the EU please contact the Data Protection Officer (dpo@accross.ac.uk).

10.Direct Marketing

Direct marketing is the communication to a particular individual of any advertising or marketing material. It is not confined to the advertising or marketing of commercial products or services. This covers all forms of communication including by post, telephone, email and other forms of electronic messages.

It is sometimes difficult to tell the difference between a **marketing email** and a **'service' email**. A service email is a communication that is sent to an individual that facilitates or completes a transaction, whether that is for the sale of goods or services. When trying to identify a service email the following questions should be asked:

- Are we under a legal obligation to send the email?
- Is the email part of the performance of a contract?
- Would the individual be at a disadvantage if they did not receive the email?

If the answer to any of these questions is 'yes' then the email is likely to be more of a services email than a marketing email. For instance an email to a student about an offer of a place on a course, paying fees or how to enrol would all be examples of service emails.

Marketing emails are those that promote the aims and objectives of the College such as information about a new course, sale of goods, services or organisational ideals. Examples would be details of how to join the sports centre which is not essential information for a student to study at the College.

Any personal details collected and held for direct marketing purposes must comply with the data protection principles e.g. it is fair and lawful, the information is only used for the purpose it is collected for, the information is kept up-to-date, it is not kept for longer than necessary and is held securely.

In addition to GDPR the Privacy and Electronic Communications Regulations 2003 (PECR) regulate in detail the use of electronic communications (e.g. email, SMS text, recorded message) as a form of marketing. PECR is due to be replaced shortly by a new ePrivacy Regulation (ePR).

There are some minor exceptions but in order to comply with the GDPR and PECR requirements governing direct marketing it is safest to assume that consent is required. Consent should normally be obtained when contact details are collected and providing an appropriate privacy notice. The consent must be 'opt-in' and any direct marketing messages should only be sent to those people who have opted in. All subsequent marketing communications that are sent should also contain an option to opt-out with details of how the individual can requests not to receive any further messages. If the College receives an opt-out request it must comply as soon as possible, there are no exceptions to this.

11.Personal Data Breaches

A personal data breach is defined in GDPR to mean:

"a breach of security leading to the accidental or unlawful destruction, loss, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;"

The College makes every effort to avoid personal data breaches, however, it is possible that mistakes will occur on occasions or things will happen that are beyond the College's control. In these cases it is important that the College responds appropriately. The College has a responsibility to deal with the breach immediately and appropriately in order to minimise the impact and prevent recurrence. GDPR also imposes a requirement that most personal data breaches are reported to the Information Commissioner's Office within 72 hours of the College becoming aware of the breach.

A personal data breach can occur for a number of reasons some examples of these include:

- Loss or theft of data or equipment on which data is stored;
- Hacking attack or inappropriate access controls allowing unauthorised use;
- Unauthorised disclosure (e.g. email sent to incorrect recipient or document posted to the wrong address or personal information posted onto the website without consent)
- Human error;

Remember that the 72 hours timeframe start from the moment any individual in the College discover that a personal data breach has occurred.

Reporting an incident

It is the responsibility of any member of staff, student or other individual who discovers a personal data breach to report it immediately as follow: Email: dpo@accross.ac.uk and during working hours call the Data Protection Officer on 01254 354004

12.Photographs and recorded images of people

Still and moving images of individuals in small groups can be defined as personal data as they feature identifiable individuals and as a result they have to be processed in accordance with the GDPR principles.

All processing of personal information is required to meet a legal justification in GDPR. In relation to photographs and recorded images this will often mean that consent is required. If you do not have the consent of the subject then consider using a different image where you know appropriate consent has been obtained.

Photographs taken for purely personal use are exempt from the GDPR requirements so photographs and videos taken by family members at a graduation ceremony are not covered by GDPR.

A sample consent form is included in Appendix 2. Copies of consent forms should be retained for as long as the image is retained for. Examples of images that are personal data are given in Appendix 3.

13.Processing Personal Data - Dos 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!"

- When you process do ensure that it is accurate, relevant and not excessive in relation to your needs.
- 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.
- 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).
- 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.
- 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.
- "Protect people's privacy and personal data like it's your own."
- 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.
- Only keep data for as long as is needed under our records retention schedule. If in doubt, please refer to the College Retention Policy.

- Ensure that all personal data is kept secure, not only from unauthorised access, but from fire and other hazards.
- 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.
- Always lock your computer when you are away from your desk. 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
- Consider the physical security of high risk personal data or sensitive information, for example use locked filing cabinets/cupboards for storage.

Appendix 1

How to handle common types of third party request for personal / sensitive information

The College should not process personal information of individuals in ways that are not covered by our privacy notices, or where there is a legal requirement, without explicit consent.

As a general rule, you should never disclose personal data to anyone other than a College staff with a legitimate work interest in the information, without consent.

1. Requests for references or confirming attendance / qualifications

The requestor should be advised that we require explicit consent from the individual concerned before we can release information (in relation to students it is important not to confirm whether or not the student has attended the College prior to consent being obtained).

The consent must be in writing (letter or email) and include sufficient information (full name, address, date of birth, dates and subjects of study/areas or work) to allow us to identify them, and be satisfied as to their identity. A letter should be signed or, for a current student or member of staff, an email from their Accrington and Rossendale College email account will be sufficient evidence of identity.

2. Requests from parents, friends or relatives

No release without explicit consent of the student.

It is acceptable to advise them that we will accept a message and, if having checked our records and such a person exists, will pass it on. This avoids disclosing any information about the student, including whether or not they are at the College.

3. Requests from organisations providing financial support

The College routinely notifies public funding bodies and the Student Loans Company of changes to a student's status. These disclosures are covered in our privacy notices and records of processing activities. Records should not be disclosed to organisations that are not covered in our privacy notices (e.g Employers) without evidence of student consent.

4. Requests from the Police or law enforcement officials

The College is not legally obliged to provide information to the police, unless presented with a court order. However, the College may choose to release information where the police, or other law enforcement agencies, can demonstrate to our satisfaction that non-release would be likely to prejudice the prevention/detection of crime or apprehension/prosecution of offenders.

The College will aim to support police investigations where possible. However, the College is obliged to manage personal information in accordance with GDPR.

Requests from the police should:

- be in writing
- be signed and counter signed, the latter by a senior officer
- be for specific information about a specific individual. While this may not always be the case, the information requested should be relevant and limited.
- state that the personal data requested are required for the stated purposes and that failure to provide the information will, in their opinion, be likely to prejudice the investigation.

The Data Protection Officer (dpo@accross.ac.uk) or in his absence the Head of Safeguarding (**Lisa Hartley**) should be informed when such requests have been received.

5. Disclosures required by law

There are circumstances where the College is legally obliged to disclose information about an individual to a third party if this is required by law, enactment or court order. All such requests should be referred to the Data Protection Officer for advice and validation.

6. Information provided for Council Tax purposes

The College routinely provides the local Councils with details of current students for Council Tax exemption purposes. Students living outside such council areas may ask for certification for this purpose and we are legally obliged to provide them with this.

Occasionally, students object to this processing and request that we do not pass their details to the Council. They are entitled to do so under the GDPR and the College would have to stop processing the information in this way unless it can be demonstrated that there are compelling legitimate grounds for processing which override the interests, rights and freedoms of the data subject.

Any objections to processing should be referred to the Data Protection Officer for advice.

7. Requests from solicitors

No release without explicit consent of the student.

Appendix 2

Photograph and Film Consent Form

I understand that Accrington and Rossendale College may wish to use photography / film footage featuring my image both internally and externally to promote the College.

This agreement applies to print and digital media format including print publications, websites, e-marketing, posters, banners, advertising, film and social media.

I give consent to the use of my photography as described above.

Signature: .....

Name: (Capitals) .....

Date: .....

Circle as appropriate: Student Staff No College connection

Address: .....

.....

.....

.....

.....

.....

Appendix 3

Examples of images that are personal data:

Where an individual is the focus of an image the image is likely to be personal data. Examples include:

1. photographs of individuals particularly those that are stored with personal details, for example, for identity passes
2. photographs of staff or students published on ProSolution, notice boards, websites
3. individual images published in a newsletter or marketing material

- **Examples of images that are not personal data:**

Where individuals are incidentally included in an image or are not the focus, the image is unlikely to contain personal data. Examples include:

- where people are incidentally included in an image or are not the focus, for example at a busy open day, the image is unlikely to classed as personal data
- images of people who are no longer alive

- **General**

  - Small Groups

Where photographs or videos are being taken of individuals or small groups of people then consent should
be obtained. This is the easiest and safest way of proving you have obtained the image fairly and in accordance with the individual's rights. There are only a small number of exceptions to this when there is an alternative legal basis for processing such as graduation ceremonies where photographs and filming are done on the basis of contract (see below).

  - *Large Groups*

It will usually be enough for the photographer to verbally ask permission to take the photograph to ensure compliance with the GDPR. Anyone not wishing to appear on a group photograph will then have the opportunity to opt out. This approach can be used when photographing, for instance, a seminar. However, if images will be posted on a website explicit consent should be sought as the image will be disclosed outside the EU.

  - *Other uses of images*

ID Cards - Photographs of staff and students are included on ID cards. This is for security purposes and consent is not required. The use of images in this way is covered in the College's Staff and Student Privacy Notices.

CCTV - CCTV cameras are located around the campus for the purposes of security and preventing and detecting crime. Notices are placed around campus advising people of the presence of these cameras.