# Personal Data Handling Guidelines for Staff

| | |
|---|---|
| Version: | v1 |
| Policy Originator Role: | Vice Principal |
| Equality Impact Assessed: | No |
| Approved by: | N/A |
| Date Approved: | N/A |
| Review Interval: | 3 Years |
| Last Review Date: | June 2018 |
| Reviewed by: | |
| Uploaded to external web site by: | Academic Registrar |
| Date uploaded: | October 2019 |
| Uploaded to intranet (SharePoint) by: | Yes |
| Date uploaded: | 2nd July 2018 |
| Next Review Date: | June 2021 |
| Audience: | Staff/ Governors/ Delivery Partners |

# Personal Data Handling Guidelines for Staff

## Context

On 25th May 2018 the General Data Protection Regulations (GDPR) became a part of UK legislation. It supersedes the Data Protection Act 1998 (DPA) and the UK's implementation of this is being referred to as the Data Protection Act 2018. The main intent of the GDPR is to give individuals more control over their personal data, impose stricter rules to companies handling it and make sure companies embrace new technology to process the influx of data produced.

All NESCOT current and new staff, who work with data of any form, are required to undertake online Educare Training, in order to become familiar with the regulation. These guidelines are to support this training in order to contextualise the GDPR to NESCOT's operations. Staff should also be familiar with the following associated policies and procedures relating to data protection which contain the full detail:

- NESCOT Data Protection Policy
- NESCOT Personal Data Breach Policy and Notification Procedure
- NESCOT Rights of Individuals Policy and Procedure
- NESCOT Records Retention Policy
- Direct Marketing Guidelines for Staff

## What information does the GDPR apply to?

### Personal data

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. The GDPR's definition is now more detailed and makes it clear that information such as an online identifier – eg an IP address – can be personal data.

The GDPR applies to both personal data held electronically and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data

For example, a name and email address is personal data as a unique individual may be identified from the information, or another example would be a name and course title. A job title and general organisational email address or phone number would not be classed as personal data as a unique individual cannot be identified.

### Sensitive personal data

The GDPR refers to sensitive personal data as "special categories of personal data". As it is more sensitive in nature it requires a higher level of protection and should only be made available to those staff who have a legitimate interest in processing the data. This means personal data about an individual's:

- race;
- ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data (where this is used for identification purposes);
- health data;
- sex life; or
- sexual orientation.

Personal data can include information relating to criminal convictions and offences. This also requires a higher level of protection.

## GDPR Principles

Under the GPDR the data protection principles set out the main responsibilities for organisations.

| | |
|---|---|
| 1 **Lawfulness, fairness and transparency** | Processed lawfully, fairly and in a transparent manner in relation to individuals. |
| 2 **Limited purposes** | Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. |
| 3 **Minimise Data** | Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. |
| 4 **Accuracy** | Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate. |
| 5 **Retention** | Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. |
| 6 **Integrity and confidentiality** | Processed in a manner that ensures appropriate security of the personal data. |

## Lawful Basis for Processing

- You must have a valid lawful basis in order to process personal data.
- Most lawful bases require that processing is ‘necessary’. If you can reasonably achieve the same purpose without the processing, you won’t have a lawful basis.
- You must determine your lawful basis before you begin processing, and you should document it. Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason.
- If you are processing special category data you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.
- If you are processing criminal conviction data or data about offences you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.
- There are 6 available lawful bases for processing. These are outlined in the table below.

| Lawful basis for processing | Detail | NESCOT Examples |
|---|---|---|
| Consent | • Consent requires a positive opt-in. Don't use pre-ticked boxes or any other method of default consent.<br>• Explicit consent requires a very clear and specific statement of consent.<br>• Be specific and 'granular' so that you get separate consent for separate things.<br>• Vague or blanket consent is not enough.<br>• Make it easy for people to withdraw consent and tell them how.<br>• Keep evidence of consent – who, when, how, and what you told people. | • Discussing progress with parents and employers,<br>• Sending marketing communications about learning opportunities and/or services. |
| Contractual | • You can rely on this lawful basis if you need to process someone's personal data:<br>• to fulfil your contractual obligations to them; or<br>• because they have asked you to do something before entering into a contract (eg provide a quote).<br>• The processing must be necessary. If you could reasonably do what they want without processing their personal data, this basis will not apply.<br>• You should document your decision to rely on this lawful basis and ensure that you can justify your reasoning. | • Staff banking details for salary payment |
| Vital interest | • You are likely to be able to rely on vital interests as your lawful basis if you need to process the personal data to protect someone's life.<br>• The processing must be necessary. If you can reasonably protect the person's vital interests in another less intrusive way, this basis will not apply.<br>• You cannot rely on vital interests for health data or other special category data if the individual is capable of giving consent, even if they refuse their consent.<br>• You should consider whether you are likely to rely on this basis, and if so document the circumstances where it will be relevant and ensure you can justify your reasoning. | you would only use this in an emergency safeguarding or medical situation. |
| Public task | • You can rely on this lawful basis if you need to process personal data:<br>o 'in the exercise of official authority'. This covers public functions and powers that are set out in law; or<br>o to perform a specific task in the public interest that is set out in law. | Sharing data with the police or other public authority in relation to a criminal investigation. |

| Lawful basis for processing | Detail | NESCOT Examples |
|---|---|---|
| | • It is most relevant to public authorities, but it can apply to any organisation that exercises official authority or carries out tasks in the public interest.<br>• You do not need a specific statutory power to process personal data, but your underlying task, function or power must have a clear basis in law.<br>• The processing must be necessary. If you could reasonably perform your tasks or exercise your powers in a less intrusive way, this lawful basis does not apply.<br>• Document your decision to rely on this basis to help you demonstrate compliance if required. You should be able to specify the relevant task, function or power, and identify its statutory or common law basis. | |
| Legitimate interests | • It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.<br>• If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests.<br>• Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority.<br>• There are three elements to the legitimate interests basis. It helps to think of this as a three-part test. You need to:<br>o identify a legitimate interest;<br>o show that the processing is necessary to achieve it; and<br>o balance it against the individual's interests, rights and freedoms.<br>• The legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.<br>• The processing must be necessary. If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.<br>• You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests. | The majority of NESCOT's data processing would come under legitimate interests.<br><br>Other examples could include providing reference for students or staff, reminder emails to former Gas Academy students to advise that their accreditation is about to expire. |
| Special category data | • Special category data is personal data which the GDPR says is more sensitive, and so needs more protection.<br>• In order to lawfully process special category data, you must identify both a lawful basis and a separate condition for processing special category data. | Out lawful basis would be legitimate interests. For students we only collect data on ethnic origin and health. |

| Lawful basis for processing | Detail | NESCOT Examples |
|---|---|---|
| | • There are ten conditions for processing special category data in the GDPR itself, but the Data Protection Act 2018 introduces additional conditions and safeguards.<br><br>• You must determine your condition for processing special category data before you begin this processing under the GDPR, and you should document it. | We have a contractual requirement to collect this data for our funding bodies the ESFA (FE) and the OfS (HE). As an organisation we would use it to monitor for Equal Opps purposes and enable use to support learning. |
| Criminal Offence Data | • To process personal data about criminal convictions or offences, you must have both a lawful basis and either legal authority or official authority for the processing.<br><br>• The GDPR deals with this type of data in a similar way to special category data, and sets out specific conditions providing lawful authority for processing it.<br><br>• You can also process this type of data if you have official authority to do so because you are processing the data in an official capacity.<br><br>• You cannot keep a comprehensive register of criminal convictions unless you do so in an official capacity.<br><br>• You must determine your condition for lawful processing of offence data (or identify your official authority for the processing) before you begin the processing, and you should document this. | • DBS Checks,<br>• declaration of unspent criminal convictions |

## General Principles for Staff

**The College's Data Protection Officer is Rob Greening, 0208 394 3241, rgreening@nescot.ac.uk**

These principles apply to staff employed in all capacities at NESCOT, including voluntary staff such as governors and those on work placements.

1. All staff will process data about students on a regular basis, when marking registers, writing reports or references, or as part of a pastoral or academic supervisory role. Nescot will ensure through registration procedures, that all students give their consent to this sort of processing, and are notified of the categories of processing, as required by the 2018 Act. The information that staff deal with on a day-to-day basis will be 'standard' and will cover categories such as:

   - General personal details such as name and address,
   - Details about class attendance, course work marks and grades and associated comments.
   - Notes of personal supervision, including matters about behaviour and discipline.

2. Information about a student's physical or mental health; sexual life; political or religious views; trade union membership or ethnicity or race is sensitive and can only be collected and processed with the students' consent. If staff need to record this information, they should use the standard College forms and systems. **Under no circumstances may this information be stored outside (e.g. on locally held spreadsheets) of the core college systems.**

   E.g.: recording information about dietary needs, for religious or health reasons prior to taking students on a field trip; recording information that a student is pregnant, as part of pastoral duties; recording information about a student's learning support needs.

3. All staff have a duty to make sure that they comply with the College's Data Protection Policy. In particular, staff must ensure that records are:
   - accurate;
   - up-to-date;
   - fair;
   - limited to what is necessary in relation to the purpose for which it is collected and used.
   - kept and disposed of safely, and in accordance with the College's Record Retention Policy.

4. Staff must seek and get specific authorisation from a designated data controller (their manager) to hold or process data that is:

   - not standard data; or
   - sensitive data (eg the sort of information described in 2 above).

   The only exception to this will be if a non-authorised staff member is satisfied that the processing of the data is necessary:

   - in the best interests of the student or staff member, or a third person, or Nescot; AND
   - he or she has either informed the authorised person of this, or has been unable to do so and processing is urgent and necessary in all the circumstances.

   This should only happen in very limited circumstances, e.g. a student is injured and unconscious, but in need of medical attention, and a staff tutor tells the hospital that the student is pregnant or a Jehovah's witness.

5. All staff are responsible for ensuring that all data that they work with is kept securely.

6. Staff must inform the Data Protection Officer of personal data breaches immediately.

7. Staff must, in the first instance, pass any data subject access requests received to the Data Protection Officer.

8. If staff feel that a particular item of Personal Data needs to be kept for more or less time than the retention period set out in the Data Retention Policy, for example because there is a requirement of law, they should contact the Data Protection Officer for guidance.

9. If staff procure any services and/or systems which require the sharing of data they must ensure that contracts are in place which contain a data sharing agreement signed by both parties.

10. Before undertaking any marketing communications staff must have approval from the Head of Marketing that such communications and source datasets are GDPR compliant.

11. Personal data must not in any circumstances be shared outside of the College unless it is encrypted and shared with a party that the College holds a valid data sharing agreement.

12. Compliance with the Data Protection Policy is the responsibility of all members of Nescot. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or access to College facilities being withdrawn, or even a criminal prosecution.

13. Assumptions should not be made. Any questions or concerns about the interpretation or operation of policies relating to data protection should be taken up with the Data Protection Officer.

## Use of Emails and SMS

Staff should be careful as to what information they include in email communications concerning other individuals. Staff should stick to factual information only and avoid communicating opinions about others. Staff should remember that at any time that copies of emails may be requested by the data subject.

The contents of emails stored on your computer systems are,of course, a form of electronic record to which the general data protection principles apply. The contents of an email should not be regarded as deleted merely because ithas been moved to a user's 'Deleted items' folder.It may be particularly difficult to find information to which a data subject access request (DSAR) relates if it is contained in emails that have been archived and removed from your 'live' systems. Nevertheless, the right of subject access is not limited to the personal data to which it would be easy for you to provide access. Subject to certain exemptions, you must provide subject access to all personal data you hold, even if it is difficult to find. You may, of course, ask the requester to give you some context that would help you find what they want. Usually, once you have found the relevant emails, the cost of supplying a copy of the personal data within them is unlikely to be prohibitive. You cannot refuse to comply with a DSAR on the basis that it would involve disproportionate effort, simply because it would be costly and time consuming to find the requested personal data held in archived emails.

SMS text messages, being electronic communications, are also covered by by the data protection principles, both college accounts and personal accounts used for communications concerning college business. This means that should a data subject submit a DSAR then such communications could be included in the scope of the request.

Staff must utilise college email accounts and SMS messaging systems for communications about a data subject, rather than using personal accounts.

# Frequently Asked Questions (Data Access)

## Can I keep my own database/spreadsheet containing student personal details?

No. It is college policy that staff do not keep and maintain their own personal databases (or spreadsheets) containing students' personal data. Storage of student personal data is limited to cross college systems. Should a staff member feel that the college systems not have the facility to store certain datasets then either the Vice Principal Planning & Information Services or the Head of Data Services should be consulted to review such datasets and their uses to see if provision for storage may be made in college systems. Should it be the case that provision is not able to be made within the core systems then the Vice Principal will review the datasets, assess data controls and security and if satisfied approve the use of the database/spreadsheet. By not complying with this you increase the risk of breaching GDPR.

It is the duty of staff to ensure that the Data Protection Officer is informed of all local data storage systems.

The appropriate core systems where information may only be stored may be seen in the table below:

| Type of personal data | System where information may only be held |
|---|---|
| Learner enrolment records and contact details | EBS & PICS |
| Employer contact details | ProEngage |
| Unit assessment tracking and monitoring data (all provision) | ProMonitor |
| Applicant records and contact details | Engage2Serve Applicant Management System / EBS |
| Apprenticeship Reviews | ProMonitor |
| Personal records relating to financial support | PayMyStudent |
| Learning Support Records | EBS/ ProMonitor |
| Other stakeholder client contact information | Sharepoint/ Outlook |

## Can I transport personal data off-site?

You should not take any student personal data off-site. This includes storage on external memory devices such as USB sticks, laptops and personal electronic devices such as mobile phones and tablets. Should staff members wish to access student personal data when off-site then the data must be stored on and accessed from the college Sharepoint site or OneDrive. When accessing such data off-site then the staff member must ensure that the data protection principles are adhered to.

Staff should avoid using public cloud storage solutions as often the servers on which data is stored may be located outside of the EEA. The DPA requires that personal data "shall not be transferred to any country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data." For example, the popular cloud storage solution, Dropbox, stores files in secure storage servers. located in data centers across the United States, and thus outside of the EEA.

## I access my work emails using my mobile phone, are there any safeguards that I need to put in place?

You must have appropriate security in place to prevent the personal data you hold from being accidently or deliberately compromised. Staff need to comply with the Staff Acceptable IT Usage Agreement. You need to take appropriate measures to protect against unauthorised or unlawful access, for example if the device is lost or stolen. Thus, you should;

- Use a strong password to secure your devices;
- Avoid downloading emails to a removable memory card, such as a micro or mini SD card;

- Ensure that access to the device is locked or data automatically deleted if an incorrect password is input too many times;
- Ensure that the device automatically locks if inactive for a period of time;
- Register devices with a remote locate and wipe facility to maintain confidentiality of the data in the event of a loss or theft;
- Make sure you have a process in place for quickly and effectively revoking access a device in event of a reported loss or theft;
- Regularly delete any email content downloaded on to the device.

## Frequently Asked Questions (Data Sharing)

### The police have contacted me requesting information to assist in a criminal investigation, what do I do?

If you have the informed consent of the individual, then you can. If you cannot gain consent or gaining it might jeopardize the investigation (e.g. evidence is destroyed), then you need to consider if there is a duty or power, in law, to share information. If there is **a legal duty then disclosure is mandatory** and consent is not necessary. If there is **a legal power, you can disclose relevant information but it is not mandatory**, however do consider seeking consent or informing the individual.

You should inform any police officer requesting information that you may need to seek consent and do they still wish you to continue? Alternatively they may be able to satisfy you that consent would not be appropriate because of the nature of the investigation (via a **section 29 exemption form**). The most likely legal basis for disclosure to the police are:

It is **preferable that the police come with a signed section 29 exemption form**, however in some circumstances we will allow them to complete a NESCOT data sharing agreement.

**Legal Duty: (You MUST disclose, even without consent)**

- **Prevention of Terrorism Act (1989) and Terrorism Act (2000)**
  If you have gained information about terrorist activity you MUST inform the police.

- **The Road Traffic Act (1988)**
  You have a statutory duty to inform the Police, when asked, the name and address of drivers who are allegedly guilty of an offence; do not disclose clinical information.

- **Court Order**
  Where the courts have made an order, you must disclose the required information, unless the organisation decides to challenge the order in court.

- **Social Security Fraud Act (2001)**
  Requires education institutions to provide any information to authorised officers of the Department for Work and Pensions or local authorities which they require for the investigation of fraud against the state benefit system. Refusal to provide the information can lead to prosecution of the institution.

**Legal Power: (You MAY disclose, but must consider implications of gaining consent)**

- **The Police and Criminal Evidence Act (1984)**
  You can pass on information to the Police, as the act creates a power to do so if you believe that someone may be seriously harmed. Serious arrestable offences include murder, rape, kidnapping and causing death by dangerous driving.

- **The Crime & Disorder Act (1998)**

Information may be required on an individual if there is a need for strategic cross-organisational planning to detect, prevent or reduce crime and disorder that an individual may be involved in. A nominated officer deals with such requests.

- **Multi Agency Public Protection (includes the Probation Service)**
  The Criminal Justice and Court Services Act 2000, sets the framework for sharing information about potentially dangerous offenders. Information about individuals may be required by 'Multi Agency Risk Conferences'. If you are requested to provide information, you should consider gaining consent/informing the individual(s) unless this may cause more harm than good. If the risk presented by an individual(s) clearly cannot be effectively managed without information and gaining consent is inadvisable, then relevant information can be shared as it is in the interests of the public.

**Where gaining consent may be prejudicial to an investigation:**
The Police may seek personal information under an exemption of the Data Protection Act. A Section 29(3) exemption is used when making enquires which are concerned with:

**a) the prevention and detection of crime or**
**b) the apprehension or prosecution of offenders**

and the view of the Police is that seeking consent or even informing the individual(s) about the transfer of data will prejudice the enquiry as they may destroy evidence or abscond. A section 29 exemption allows information to be provided by organisations without gaining consent.

- The Police will need to produce a Section 29(3) form requesting the information, signed by a Police Inspector who has decided to serve the exemption.

- You do not have to supply information, you may still seek consent/inform, however the Police have made a considered judgement about their need for information.

- Do not feel pressurised to give information because the police have requested it. It is reasonable to ask why it is needed and what is required before making a decision.

**Children in Need - Legislation:**
Under section 47 of the Children Act (1989) a Local Authority, working with other relevant agencies, must make all necessary enquiries to decide whether they should take any action to safeguard or promote a child's welfare. In such a situation, firstly confirm it is a section 47 enquiry and then release relevant information, unless 'to do so would be unreasonable in the circumstances of the case'. You do not have to gain consent of the parent or child or inform them.

If you suspect a child is being abused, but there is no request for information, you have a legal power to disclose information to Social Services (under 'vital interest' & 'medical purpose' conditions of the Data Protection Act) and/or the Police (under the Police & Criminal Evidence Act). Consider whether gaining consent or informing the child and parents would be beneficial or detrimental to the situation. If detrimental then disclosure without consent is permitted.

**Emergency Situations**
An emergency situation is one where we have reason to believe that there is a danger of death or injury to a member of the College or any other person. The police and other emergency services may urgently require personal data from us, and may not have time to complete a formal written request. In these circumstances, any staff member who has access to the data can legally disclose the information, but the safeguards below need to be met:

1. If possible, seek the authorisation of a senior manager before providing the data.

2. If the request is received by telephone, ask the caller to provide a switchboard number, and call them back through the organisation's switchboard before providing the data. This provides a basic (though not foolproof) way of checking that the call is genuine.

3. Ask the enquirer to follow up their request with a formal written request, so that we have this on

file. Keep a record of the enquiry and your response, and pass details to the Data Protection Officer as soon as possible.

4. Do not be bullied into disclosing data if you have any doubt as to the validity of the request. Ask the enquirer to submit the request in writing, and refer the enquiry to those staff who normally deal with written requests

## A parent phones to ask me for information about a student. Am I able to release information to them?

Unlike schools who have specific obligations to disclose a pupil's educational record to a parent by virtue of The Education (Pupil Information) (England) Regulations 2005 the position for college students is less clear.

By signing the consent during enrolment students aged 18 years have given permission for the college to share information on their academic progress with their legal guardian(s). Staff should look up the student's record on EBS OnTrack to ensure that consent has been given.

Staff must be able to ensure that the person making the request is actually the parent/legal guardian so you will need to identify them in some way before you can give out any information. You can advise them that you need to verify their identity before you are allowed to share any information so you could advise that you will call them back using the "next of kin" number on the student record as for students aged under 19 years this should be the primary carer's number.

Where the parents are divorced then information on academic progress may only be shared with the parent who has custody of the child. Information may only be released to the other parent should the student give explicit consent for us to share with this parent. If in doubt to do not give out the information as disclosure could compromise the students' safety.

If sensitive personal data is involved (such as that relating to a disability, race, ethnic origin, health etc) then the conditions for disclosure are even more robust e.g. explicit consent is required, or disclosure is necessary to protect the vital interests of the student. Should the there be any concerns that the release of information would compromise the safety or well-being of the student then the information should be withheld.

## I receive a data subject access request what should I do?

Data subject access requests are managed by the Data Protection Officer. You should **immediately** first direct the person requesting the information to the form on the college website as they will have to submit evidence of their identification with their request. The form is located from the **Privacy** item in **the About Us** menu option.

On receipt of the completed form and evidence of identity the Data Protection Officer will manage the process in line with our Rights of Individuals Policy and Procedure.

We have only one month to respond to such requests.

## How will the College be collecting consents under the GDPR?

The college will collect the following consents from every student during the enrolment process:

- Consent for NESCOT to send marketing communications
- Consent for NESCOT to discuss learner progress with employers
- Consent for NESCOT to discuss learner progress with parents/legal guardians (mandatory condition of enrolment for learners aged under 19)
- Consent for NESCOT to contact the Student Loans Company in relation to loans applications
- Consent to be contacted by the ESFA for the purposes of marketing or surveys.

- Consent to be contacted by the Office for Students for surveys.

The Learning Support and Student Welfare Teams will collect consents to share data and discuss learners' progress with social/key workers, external agencies and local authorities.

The Employer Services Team will need to collect and record consents for marketing communications from employers in the course of engagement.

For any other activities where you wish to collect consent to send out marketing communications you will need to refer directly to the Data Protection Officer for advice.

The necessary consents need to be recorded in EBS or ProEngage, whichever is the most appropriate, including preferred method of contact, date consent was given and how the consent was given.

## What should I do if I become aware of a personal data breach?

A personal data breach is: "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service".

In the event that you have been made aware of a personal data breach then you must immediately notify the Data Protection Officer who will follow our Personal Data Breach Policy and Notification Procedure commence an investigation. Our DPO will only have 72 hours to complete an investigation and notify the Information Commissioners Office (ICO).

## Are confidential references subject to data access requests?

From time to time you may give or receive references about an individual, eg in connection with their employment, or for educational purposes. Such references are often given 'in confidence', but that fact alone does not mean the personal data included in the reference is exempt from subject access.

The DPA distinguishes between references you give and references you receive. References you give are exempt from subject access if you give them in confidence and for the purposes of an individual's education, training or employment or the provision of a service by them.

**There is no such exemption for references you receive from a third party. I**f you receive a DSAR relating to such a reference, you must apply the usual principles about subject access to decide whether to provide some or all of the information contained in the reference.

**Example**
Company A provides an employment reference for one of its employees to company B. If the employee makes a SAR to company A, the reference will be exempt from disclosure. If the employee makes the request to company B, the reference is not automatically exempt from disclosure and the usual subject access rules apply.

So as the example shows although there is no requirement for you to disclose the contents of a reference that you have provided the data subject could request the disclosure from the entity that you have provided the reference to. Thus, staff should ensure that the content of any reference contains only factual information that can be evidenced if challenged and avoid any opinions that cannot be clearly evidenced.

## If a company approaches us for a reference for a former student, do we have to contact the former student to request consent?

No. By providing the College as a referee the former student has given consent to the employer. There is a legitimate interest in providing the reference to the company as it would be in the best interests of the former student.

## I am in the process of procuring a new cloud-based system which requires access to our student data, what should I do to ensure compliance with GDPR?

The GDPR requires us to have a contract in place with the supplier that contains clauses relating to data sharing, data processing, data retention and data security. All contracts must be passed to the College Procurement & Contracts Officer to ensure contract compliance before passing the contract to the Deputy Principal for signature.

## I need to share data with an external agency/authority/awarding body/service provider, what should I do to ensure compliance with GDPR?

In the first instance you must seek approval from the Data Protection that the data sharing is permissible under the GDPR. You would then need to request that a Data Sharing Agreement drawn up between both organisations (most organisations should have their own templates for these). These agreements must contain clauses relating to data sharing, data processing, data retention and data security. All agreements must be passed to the College Procurement & Contracts Officer to ensure contract compliance before passing the contract to the Deputy Principal for signature.

## An employer phones to ask me for information about an apprentice. Am I able to release information to them?

Only if we have the learner has provided consent and we have it recorded on our system.

## I am required to share information with an external agency or local authority, what should I have in place to allow this?

You should have in place signed consent for sharing from the student or if the student has severe learning difficulties from their parent/legal guardian. You must also have in place a data sharing agreement with that agency or local authority. These data sharing agreements need to be passed in the first instance to our Procurement & Contracts Officer who will review before passing them to the Deputy Principal for signature. The Deputy Principal will returned signed copies to yourself, the Data Protection Officer and the Procurement & Contracts Officer.

## How do I share personal and sensitive information outside of the College?

Before you share personal data you must ensure you have a data sharing agreement in place and the relevant consent or in lieu of consent the relevant lawful basis for sharing. Information must be in an encrypted format. You can send the information via the EGRESS email system, a secure file sharing system, encrypted PDF or encrypted zip file. Password should always be send in a separate email. You are using a file sharing system then you must ensure that the servers for the system are located in the EEA. For example, DropBox is hosted in the USA and as such is not permissible to use.

## A third party has asked me to share someone`s contact details. Can I share?

You may only share if you have the permission of the person whose details you intend to share.

# Frequently Asked Questions (Communications)

### Are “keep warm communications” to applicants classed as marketing communications?

No. Applicants are classed as existing customers who are in the process of procuring a service from us. Such communications are part of the application process and thus the service that they subscribed to.

### I do not have consents to contact past employers/clients, how do I get around this, to send out marketing communications?

If the employer/client is an existing customer, that it is someone to who you are currently providing a service or are negotiating providing a service then you can still send them marketing communications but must provide them with the ability to unsubscribe from such communications.

For any past employers/clients for whom you do not have consents given post the introduction of GDPR (25th May 2018) you cannot send them marketing communications. However, you can look up the general address, telephone number or organisation email address for the company on their website and send a communication, direct to say the HR Manager or CEO. As you are not using personal data this falls outside of the GDPR.

Full details on direct marketing communications may be found in the Direct Marketing Guidelines for Staff

### I would like to send out a marketing communication. What should I do to ensure GDPR compliance?

Ensure that the data you have sourced is from one of the central college systems only as that will be where consents are held. If sourcing data from MIS they will ensure that the consent fields are including in the data exports so you can strip out any records where consent has not been given. You then need to share your communication and information on your data source with the Head of Marketing, who will grant approval or provide feedback on how to ensure that the communication is both appropriate and GDPR compliant.

### I sometimes record casual, unprofessional comments about staff or students in emails and on ProMonitor. Are there any implications?

Yes, there certainly are implications. Should a student or staff member submit a data subject access request then the College is legally obliged to share all of the information that we hold about them. This would include any emails in which they are named (redacted so as not to disclosed third party information) and **all records from all systems**, so comments (including “confidential comments” on ProMonitor would be included. If you wish to make comments to a colleague that you would never like a student to see then I suggest that you do this verbally.

## Frequently Asked Questions (Data Currency)

### A student or staff member wishing to update their personal details on our systems. How do they do this?

Please direct them to the Change of Details Request Form on the college website. The form is located from the Privacy item in the About Us menu option. Our Data Services Team will progress the change in line with our Rights of Individuals Policy and Procedure.

## Frequently Asked Questions (Data Security/Storage)

### We keep student work files and portfolios in our staff office on shelves, is that permissible?

With such files it is not always possible due to volumes to lock these away. At the very least staff must ensure that if they are the only person in the office that they ensure that the door is locked when they leave.

### When I leave my shared office can I leave my PC on?

Depending on the duration you will be out of the office the PC should either be fully shutdown or the screen lock in place when you leave the office.

### We keep paper copies of forms that contain personal information is that fine?

The College is actively progressing to paperless working. We should avoid having paper files as there is a higher risk of a data breach or data loss. All of the college systems facilitate scanning and uploading of paper records. All paperwork relating to student records should be uploaded against the student record in EBS. ProMonitor (student tracking), ProEngage (CRM), Engage2Serve (applications), Resource (finance) and CIPHR (staff records) have this facility. We also have Filestream and Sharepoint as electronic document storage solutions. If you are unsure of where to store your electronic documents please contact the Head of Data Services for advice. Once scanned all paper copies must be securely disposed off.

If for any reason you cannot avoid having paper files then you need to make provision to ensure that these files are securely stored and only accessible by authorised staff.

To ensure minimum risk managers should put in place a Clear Desk Policy to ensure that all personal data is locked away at the end of the day and not lft on desks or in-trays. Managers will also be accountable in the event of a data breach by a member of their staff if they have not put in place appropriate safeguards.

All paper files relating to student records my only be stored in the CIS Data Services office.

### How do I securely dispose of paper records?

The GDPR is very explicit about disposal of information. Any documentation that contains personal data must be disposed of securely. All managers must at the end of the academic year review the retention schedule for the data that the hold and ensure that provision is made promptly for secure disposal. In the first instance documentation should be shredded (shredder is located in the LRC). If this is no feasible then staff should obtain secure disposal sacks from the Facilities Manager, being mindful that the college has to pay a fee for the disposal of each sack.

Filled secure disposal sacks must be securely locked away until collected by the disposal company.

Please see the College's Record Retention Policy.

## What is the process for deletion of electronic records?

Electronic records must be deleted in line with the Record Retention Policy. Managers are responsible for ensuring that records for their areas stored on Sharepoint, network drives or Filestream are deleted once their retention period has expired. Each of our core management information systems has an "owner". The owner is responsible for working with software suppliers to ensure record deletion, once the retention schedule has expired.

| System | "Owner" |
|---|---|
| EBS Student Record System | Head of Data Services |
| PICS Apprenticeship MI System | Head of Data Services |
| Engage2Serve Applicant Management System | Head of Advice & Guidance |
| ProMonitor | Director of PDBW |
| ProEngage | Head of Business Development |
| ProAchieve | Head of Data Services |
| ATLAS / EBS Learning Support | Director of Student Support |
| Horizon Library Loans System | Head of Learning Resources |
| Resource | Head of Finance |
| PayMyStudent | Student Finance Officer |
| BKSB | MathsTeam Manager |
| CIPHR | Director of Human Resources |
| START Careers Management | Head of Advice & Guidance |

## How do I archive my records?

Paper records should be scanned and stored the appropriate system or location. Sometimes this will not always be feasible. In such instances where a physical archive is required then this must be appropriately managed. Some rules to follow:

- Your archive must be in a secure location where only authorised members of your team have access. It should have more secure access than being in a location that is secured by only a "general college key".

- You must have a log book to record the contents of your archiving. So essentially nature of records, date archived, archived by, date due for disposal and date actually disposed. This will make it easier for future data protection audits.

- Archived records should only be stored in archiving boxes or archiving bags, clearly labelled with content, date archived and date when due for disposal.

- Archives must be well ordered, with the most recent archiving located at the back and the oldest at the front. This will greatly assist the disposal process.

- You must at all times know the location and status of your archived records.