![BU_Core_CMYKportraitsml [Converted]]()

**Owner:** Legal Services

**Version number:** 9

**Approved by:** University Leadership Team

**Date of last review:** February 2024

**Due for review:** 1 year from last review

**DATA PROTECTION POLICY**

1. **Purpose**
	1. This policy concerns Bournemouth University Higher Education Corporation's (**BU's**) obligations under the **Data Protection Legislation[[1]](#footnote-1)** The purpose of the Data Protection Legislation is to safeguard personal information (called **Personal Data** in the Data Protection Legislation and defined at section 6 below). Personal data is information relating to living individuals who:
* can be identified or who are identifiable, directly from the information in question; or
* who can be indirectly identified from that information in combination with other information held by BU.
	1. Information may be identifiable because it includes or is linked to a unique identifier or label such as a name or ID number, or because it comprises several fields or characteristics which together enable identification of the individual even though they are not linked to a name or ID number. Other information may also be regarded as identifiable in certain circumstances, such as an IP address or a website cookie identifier.
1. **Who does this policy apply to?**
	1. This policy is intended to ensure that all staff and other relevant individuals who process Personal Data for BU purposes or have access to BU systems are properly informed about BU's obligations under the Data Protection Legislation and their role in enabling BU to comply with those obligations.

* 1. It applies to:
		1. all employees of BU and its wholly-owned subsidiary entities, whether permanent or temporary, and workers, casual and agency staff when working in or for BU (**Staff**);
		2. all postgraduate research students of BU, in respect of Personal Data they process for the purposes of, or in the course of carrying out, their BU programme of study (**PGR Students**);
		3. all of the following (together, **External Members**):
* all external members of the BU Board when acting in that capacity;
* all directors or trustees of BU's wholly owned subsidiary companies; and
	+ 1. other individuals given authorised access to Personal Data for the purposes of activities they perform for or on behalf of BU, where and to the extent that this is specified in the terms of their authorisation. This may include volunteers, visitors, contracted service providers and external members of BU Faculties or committees (**Authorised Third Parties**).

* 1. If you have any questions or concerns about this policy or about data protection generally, please use the email address dpo@bournemouth.ac.uk.
1. **ABOUT THIS POLICY AND WHY IT IS IMPORTANT**
	1. Data protection is important because it seeks to protect individuals' privacy rights and requires their personal information to be used in a fair and lawful manner. The Data Protection Legislation is enforced by a national regulator, the Information Commissioner’s Office (“ICO”), and by the courts. A breach of the Data Protection Legislation could have serious consequences for the individuals whose Personal Data is affected, as well as for BU – including legal action against BU and/or damage to BU's reputation.
	2. Individuals failing to comply with Data Protection Legislation can, in certain circumstances, face criminal liability. Breach of this policy and its associated procedures in force from time to time, may result in other actions or sanctions as follows:
		1. for Staff and PGR Students this may constitute a disciplinary offence and will be subject to investigation under the relevant BU disciplinary procedures;
		2. For External Members and Authorised Third Parties, breach of this policy and its associated procedures in force from time to time, may result in other contractual or legal sanctions.
	3. This policy is intended to give an overview of BU's obligations under the Data Protection Legislation and sets out the core principles which need to be applied to ensure that BU complies with the Data Protection Legislation. This policy gives a number of links to other policies and processes and to guidance hosted on the BU [Data Protection SharePoint site](https://livebournemouthac.sharepoint.com/sites/DataProtection) which provides more detailed information on how to apply in practice the core principles stated in this policy. It is essential that you use these links when they are relevant to you and your activities relating to Personal Data, to ensure you comply fully with this policy. Data protection is relevant to many different aspects of BU’s activities and it is not workable to state all detailed requirements in a single policy document. Those covered by this policy are expected to access additional processes, policies and guidance which are referred to in this policy where these are relevant to activity they are undertaking. In applying this policy and determining whether an individual has complied with it, BU will consider the content of those materials, and whether the individual was or should have been aware of their content.
2. **KEY DATA PROTECTION ACTIONS & RESPONSIBILITIES**
	1. This section sets out a summary of the steps which those subject to this policy should take to fulfil their data protection responsibilities. Some of these steps are less likely to be relevant in practice for those who do not have management or decision-making responsibilities, but is still important to understand the principles which apply when decisions are made about processing of Personal Data:
		1. Mandatory Training: Undertake mandatory information governance training within the required timescale. (This does not apply to all External Members or staff of BU’s wholly-owned subsidiaries; if you fall into these categories, you will be told if you need to undertake the training)
		2. Processing Personal Data: Be aware of when, where and why, both practically and in terms of legal basis, Personal Data is being processed and the need to comply with the Data Protection Legislation. Be particularly cautious about processing special category data (previously “sensitive personal data”) or recording comments about individuals. Remember, that just because you can access or view Personal Data does not necessarily mean that you should do so.
		3. Apply “data minimisation”: Only process the minimum Personal Data necessary for a particular purpose.
		4. [Protect Personal Data](https://livebournemouthac.sharepoint.com/sites/DataProtection/SitePages/KB-Information-Security.aspx): Apply available data security tools and measures, such as encryption and pseudonymisation, to protect Personal Data from unauthorised access or disclosure. This applies to storage, use and destruction/deletion of Personal Data, and also understanding, and taking reasonable steps to avoid, common methods of triggering cyber/data security attacks. For managers: make sure that your team is aware of the controls, measures, policies and tools used within your team.
		5. Data Breach Reporting: Promptly report any actual, suspected or potential breach of data security or of the Data Protection Policy, including “near misses”, following the reporting lines set out [here](https://livebournemouthac.sharepoint.com/sites/DataProtection/SitePages/Personal-Data-Breach.aspx).
		6. New processing activities: If you are involved in planning or decisions about new processing activity (i.e. a new use of Personal Data), as a project team consider carrying out a [Privacy Impact Assessment (“](https://livebournemouthac.sharepoint.com/sites/DataProtection/SitePages/Privacy-Impact-Assessments.aspx)**[PIA](https://livebournemouthac.sharepoint.com/sites/DataProtection/SitePages/Privacy-Impact-Assessments.aspx)**[”)](https://livebournemouthac.sharepoint.com/sites/DataProtection/SitePages/Privacy-Impact-Assessments.aspx) and ensure that these questions are asked and answered:
* Do we need to use Personal Data at all?
* Have individuals already been told about this use of their data?
* Is there a clear legal basis for the processing (i.e. applicable conditions of processing have been identified)?
* What arrangements or controls need to be put in place before you start processing, to ensure data minimisation and data security?
	+ 1. Existing processing activities:
* Be aware that your handling of Personal Data must be consistent with relevant [privacy notices](https://livebournemouthac.sharepoint.com/sites/DataProtection/SitePages/BU-Privacy-notices.aspx);
* Be aware of the basis for processing Personal Data, in particular whether it relies on the individuals’ consent and the scope of any consent;
* Follow any established processes or practices within your team regarding when, how and by whom the Personal Data should be used, unless you have reason to think that this approach is inappropriate. Managers should ensure that these are identified to staff during induction. Do not depart from standard process without seeking advice.
	+ 1. Sharing or transferring Personal Data: Be cautious. Be clear about the purpose of the sharing and only disclose what is necessary for that purpose. Except in a true emergency:
* Only share within BU if the recipient needs the Data for a clearly-defined purpose within the uses described in the relevant privacy notice and in accordance with established practice.
* Only share outside BU if you are following an established process or practice (see above) or after seeking appropriate advice. BU needs to do “due diligence” (appropriate checks) on the recipients of Personal Data to ensure it will be appropriately safeguarded.
	+ 1. [Data Retention:](https://livebournemouthac.sharepoint.com/sites/DataProtection/SitePages/KB-Data-Retention.aspx) Only keep Personal Data where needed for a defined purpose (including any legal and audit requirements) and in accordance with BU or departmental retention policy or process – but seek appropriate advice before destroying or deleting materials unless the deletion is clearly provided for in a relevant retention policy/process.
		2. **Respond promptly** to requests for information or assistance with PIAs, data audits, subject access requests, data breach investigations and other data protection queries or issues.
		3. **Seek advice about new processing activities or if in any doubt about data protection issues.**
	1. In taking these steps you may require support or advice from others within BU, in particular the Data Protection Officer (dpo@bournemouth.ac.uk), Legal Services (legalservices@bournemouth.ac.uk) or IT Services. You should never hesitate to seek advice if you have any doubts or concerns about the handling of Personal Data by yourself or others, or technical questions about IT tools or processes.
	2. Aside from completion of mandatory training, the steps required to be taken by PGR Students under this Policy will depend on the nature of the research they are undertaking. As part of the preparation of a Research Data Management Plan in accordance with BU’s Research Data Policy, PGR Students should identify the extent to which their research involves processing Personal Data and the arrangements for managing that Data in accordance with this Policy. In making those arrangements PGR Students must seek advice from their supervisors and others in BU as required. Supervisors must work with their PGR Students to identify any needs for training and guidance round data protection, and to help them access required resources, support, training and guidance for these purposes.
1. **REPORTING DATA BREACHES AND BREACHES OF THIS POLICY**
	1. A data breach is a situation in which there has been accidental or deliberate unlawful destruction, loss, alteration, unauthorised disclosure of or unauthorised access to Personal Data. A data breach may result in disclosure/risk of disclosure of BU Personal Data to third parties, but can also occur within BU when Personal Data is made available to unauthorised persons or used inappropriately.
	2. A “near miss” of a data breach is a situation in which a data breach was close to taking place but was avoided by ad hoc intervention (rather than standard application of policy or process).
	3. BU has a legal duty to notify the ICO of certain data breaches within tight timescales and take immediate action to investigate and respond to any suspected data breaches. BU must respond to any “near miss” with a view to preventing a future data breach.
	4. Staff, PGR Students and External Members must therefore immediately report any definite or suspected data breach or near miss in accordance with the reporting lines set out [here](https://livebournemouthac.sharepoint.com/sites/DataProtection/SitePages/Personal-Data-Breach.aspx).
	5. BU will identify, manage and report on Data Breaches and near misses in line with ICO guidance, BU Information Security Incident Management processes, and the BU Major Incident Plan. These processes assign responsibility for notifying data breaches, e.g., to data subjects and/or the ICO. Further information can be found [here](https://livebournemouthac.sharepoint.com/sites/DataProtection/SitePages/Personal-Data-Breach.aspx). Staff to whom this policy applies should not make such notifications without express authority to do so.
2. **DEFINITIONS**
	1. The terms used in the policy (including personal data, special category data, data subjects, Data Processor, Data Controller, processing, data minimisation, anonymization and pseudonymisation) have the meaning given to them by the Data Protection Legislation. They are explained in this guidance available on the [DP SharePoint site](https://livebournemouthac.sharepoint.com/sites/DataProtection/SitePages/KB-Definitions.aspx) and through the mandatory training modules. If you need further support in understanding the scope or application of the policy, contact the DPO or Legal Services.
3. **DATA PROTECTION ROLES AND RESPONSIBILITIES AT BU**
	1. BU is responsible for complying with the Data Protection Legislation. Usually, this responsibility is as a Data Controller, although BU may also, in certain circumstances, process Personal Data on behalf of a third party, in which case BU will have responsibility as a Data Processor.
	2. The Board of Governors has delegated day-to-day responsibility for compliance with the Data Protection Legislation to the Chief Operating Officer.
	3. Deans of Faculties and Directors/Heads of Professional Services will be responsible for data protection within their area of business and directly accountable to the CIO and BU board for findings in non-compliance to this policy
	4. Further information on the governance structures and specific Information Governance roles within the University can be found [here](https://livebournemouthac.sharepoint.com/sites/DataProtection/SitePages/Accountability.aspx). These drive the implementation of the BU Data Protection management framework which helps to embed accountability measures and create a culture of appropriate privacy protection across the organisation.
	5. All those outlined in section 2 are responsible for complying with this Policy, where it is relevant to their role within BU or the work they are conducting at, for, or in association with BU. This includes adopting the process and procedures which support this Policy which are relevant to them and their activities at or for BU and promptly passing on communications or escalating issues where required. For managers, their responsibilities include taking appropriate steps to ensure those they line manage comply with this Policy.

* 1. It is mandatory for all Staff and PGRs (and for others covered by this Policy who are notified accordingly) to undertake modules of information governance training which are notified to them as mandatory. These requirements may include training as part of induction programmes and additional and/or refresher training modules. Failure to undertake training notified to you as mandatory within the specified timescales without good reason will be treated as a disciplinary matter for staff and PGRs and for others covered by this Policy may result in actions or sanctions as referenced in section 3.2.
	2. As required by the Data Protection Legislation, BU has an appointed Data Protection Officer (“**DPO**”). The DPO is responsible for fulfilling the statutory requirements of the DPO role and must be involved in all matters and issues which relate to the protection of Personal Data within BU as soon as possible (dpo@bournemouth.ac.uk). BU’s Information Office is a service provided by Legal Services which supports and works closely with the DPO. The Information Office provides advice on the Data Protection Legislation to Staff and BU’s Board Members, acting in their capacity as such. It also manages BU’s response to subject access requests and supports the DPO in managing requests from Data Subjects to exercise their other rights under the Data Protection Legislation.
1. **DATA PROTECTION PRINCIPLES**
	1. The Data Protection Legislation is built around several data protection principles). This policy and its associated policies, processes and guidance are all intended to ensure BU’s compliance with these principles. Those subject to this policy need to be aware of the principles and what they mean for them in practice when they are processing Personal Data. Further information is available here on the DP [SharePoint site](https://livebournemouthac.sharepoint.com/sites/DataProtection/SitePages/Definitions---Principles.aspx). If you need further support in understanding or applying the principles, please contact the DPO or Legal Services
2. **DECIDING TO COLLECT OR USE PERSONAL DATA**
	1. If you are involved in a decision or planning an activity which would result in Personal Data being processed for a particular purpose for the first time, you must consider the following questions:
* Do you need to use Personal Data at all? Can you achieve the same purpose without using identifiable data?
* Have the Data Subjects already been told about this use of their Personal Data, or will you need to inform them about it? (See section 10 on Privacy Notices below)
* Does the processing fall within relevant conditions of processing in the Data Protection Legislation? (See section 11 on Lawful Grounds of Processing below)
* What controls need to be put in place before you start processing this Personal Data, to ensure that BU is applying data minimisation and meeting its data security obligations? (See section 16 on Data Security below, and you should always refer to the [BU Information Classification Policy / guidance](https://staffintranet.bournemouth.ac.uk/workingatbu/informationsecuritydataprotection/informationsecurity/iwantto/classifyinformation/))
* Have you completed the initial [Privacy Impact questionnaire](https://livebournemouthac.sharepoint.com/sites/DataProtection/SitePages/Privacy-Impact-Assessments.aspx)? Should you carry out a full PIA (details here: [PIA on SharePoint](https://livebournemouthac.sharepoint.com/sites/DataProtection/SitePages/Privacy-Impact-Assessments.aspx))?

These questions apply whether:

* you are going to be collecting or receiving particular types of Personal Data for the first time;
* you are going to be using Personal Data which BU already holds in a new way or for a new purpose;
* you are considering using a new system or IT tool to process Personal Data; or
* you are using existing systems or tools to Process Personal Data in a new way.
	1. A PIA is a risk assessment tool which enables you to identify:
* the potential impact of processing on individuals and on BU;
* the legal basis for the processing; and
* actions to reduce adverse impact and control privacy risks.

A PIA is relevant both to proposals regarding Personal Data within BU and to data sharing proposals and any other third party relationship or arrangement which involves data processing of any kind. Examples of the latter would be research collaboration, procurement of services or management of joint events..

* 1. There is a legal requirement to carry out a PIA in some circumstances. BU operates a [PIA process](https://livebournemouthac.sharepoint.com/%3Aw%3A/s/DataProtection/EW7UBWmLClZPu3ywLGxY-qQB47Up-Z3-qpkOgw5lxMPBpQ?e=EAiBWe) which is intended to ensure that we meet this legal requirement but also to fulfil a wider role in helping us manage data protection risks appropriately.
	2. The PIA process must be followed where:
* you are submitting a proposal for Business Case Approval;
* you are submitting a proposal for research ethics approval;
* you are preparing any other proposal for activity which would involve new processing of Personal Data, either through collecting/receiving certain Personal Data for the first time, sharing it within BU or with a third party for the first time and/or using Personal Data already held within BU for a new purpose.

9.5 In all of these circumstances you must complete the questionnaire which is the first part of the BU PIA process. This must be done before, and submitted with, any request for internal approval or sign-off of the relevant proposals. Depending on the outcome of the questionnaire, you may also be required to complete a full PIA and implement the action plan which is the output of the PIA. When following the PIA process, use the guidance available to you [here](https://livebournemouthac.sharepoint.com/%3Aw%3A/s/DataProtection/EW7UBWmLClZPu3ywLGxY-qQB47Up-Z3-qpkOgw5lxMPBpQ?e=EAiBWe) and seek advice from the DPO as required

1. **PRIVACY NOTICES**
	1. If BU obtains Personal Data (whether from the Data Subject themselves or from a third party) it must ensure that the Data Subject is told what information will be collected, what it will be used for, which third parties (if any) it will be shared with and anything else which might be relevant to the particular purpose. This applies regardless of whether we are relying on individuals’ consent as the legal basis for processing their Personal Data. This information usually has to be provided before or at the time that information is first collected from individuals or first processed for a particular purpose. Documents which set out this information are often called Privacy Notices.
	2. All BU processing of Personal Data must be covered by one or more of the following types of privacy notice:
		1. One of BU’s core Privacy Notices which provide an overview of how we Process Personal Data relating to particular groups of individuals (e.g. Students, Staff and Applicants, Research Participants). These are held centrally on the [BU website](https://www.bournemouth.ac.uk/about/governance/access-information/data-protection-privacy) and also accessible via the SharePoint site [here](https://livebournemouthac.sharepoint.com/sites/DataProtection/SitePages/BU-Privacy-notices.aspx)
		2. Privacy Notices which are, as appropriate, specific to particular activities or engagements. For example, research participants must be given access to both BU’s general Research Participant privacy notice and project-specific information, something normally done through using the template participant information sheet.
	3. If you are using, or are about to use, Personal Data and are in any doubt about whether the use is covered by an existing Privacy Notice, contact BU’s Information Office (dpo@bournemouth.ac.uk) for advice.
2. **LAWFUL GROUNDS FOR PROCESSING PERSONAL DATA**
	1. In most cases, any processing of Personal Data will only be lawful if at least one of the following conditions is met:
		1. the individual has consented to the processing. There are significant limitations on the ability of BU to rely on consent as a basis of processing and on the way in which Personal Data collected on this basis can be processed. Please read section 12 below before proceeding to rely on consent;
		2. the processing is necessary:
* to perform a contract which the individual has entered into;
* to take steps at the request of the individual to enter into a contract;
* to comply with a legal obligation that applies to BU (except an obligation imposed by a contract);
* to protect an individual's "vital interests": this could be either the Data Subject or another individual.

Note this condition is very narrow and only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident;

* for performing a task carried out in the public interest or in the exercise of official authority vested in BU; or
* for legitimate interests of BU or a third party, except where such interests are overridden by the interests or rights and freedoms of the Data Subject, i.e. the legitimate interests are outweighed by privacy risks or impact to individual Data Subjects.

If relying on this condition, you must clearly identify the specific legitimate interest(s) you are pursuing and explain how you have balanced these against the interests of the individuals.

* 1. Public tasks: many of BU’s core activities will fall within this condition, on the basis that delivering core teaching, facilitating learning and undertaking research are public tasks or functions undertaken by universities. If you are considering relying on this condition, you need to clearly identify which aspect of BU’s public task you are pursuing, i.e. which element or activity within its core functions. You need to be aware that many BU activities will not fall within this condition, even though they may be carried out by most or all universities, if they are additional or supplementary to the core university functions (for example provision of supplementary services to students in relation to accommodation or sport/leisure). For such activities you will need to identify an alternative condition, such as legitimate interests or necessary for the performance of a contract.
	2. BU’s [Research Ethics Code of Practice](https://intranetsp.bournemouth.ac.uk/documentsrep/8B-research-ethics-code-of-practice.pdf) contains detailed information about the legal basis for processing data for research purposes, and the distinction between this legal basis and the ethical requirement to seek and record the consent of individuals to their participation in research activities.
	3. Legitimate interests: BU may be processing Personal Data because this is necessary for the purposes of its own legitimate interests (for example, its commercial interests in carrying out fundraising activities or its interests in maximising its appeal to students by providing a full range of supplementary activities and services) or the legitimate interests of the third party that the information is disclosed to.

If you are considering relying on this condition:

* you need to clearly identify the interest that is being pursued through the processing and why you consider it to be legitimate;
* a 'balancing exercise' must be carried out, weighing up the rights and interests of the individual against BU’s or the third party recipient’s legitimate interests; and
* this condition will not apply where the processing cannot be justified in light of the impact on individuals;
	1. Identifying potentially relevant conditions and deciding whether they apply to your intended processing can be a difficult and complex exercise. When planning new activities you should take advice from the DPO or the Information Office to ensure that the processing will be lawful. However your input will also be essential to determining the basis of the processing, as you will have key information about the Personal Data, the purpose of the processing, and how it would be carried out in practice.
	2. Other than consent, the conditions listed above only apply where processing of Personal Data is *necessary* for the particular purpose. They do not apply where using Personal Data for that purpose is merely easier or a “nice to have”. When considering whether/on what basis to process personal data, it is important to be rigorous in considering whether use is really necessary and identify the obstacles which prevent you from undertaking the relevant activity or achieving the relevant aim without using Personal Data. As explained above, you should also apply the principle of data minimisation to limit the amount of Personal Data used and ensure use is appropriately controlled.
	3. **Special category data** (see 4.1.2 and 6.1). To process special category data it is usually not sufficient just to identify a condition from the list above: there are additional duties – and some different lawful grounds.
	4. In many cases, explicit consent of the individual will be needed to process special category data (see section 12.4 for more on the meaning of “explicit” in this context). The Data Protection Legislation does, however, provide some alternative lawful grounds for processing special category data. Applying any of the lawful grounds to BU's processing of this data activities requires careful thought.
	5. You should seek advice from BU’s Information Office if you intend to process special category data. Where the processing relates to special category data about Staff, BU’s Information Office will consult with Human Resources. In any event, you need to inform the DPO where the processing of special category data is to take place.
1. **consent**
	1. If properly obtained, consent provides a very clear legal basis for processing. However there are certain requirements which must be met for consent to be valid and for BU to be able to rely on consent on an on-going basis. In particular:
* the request for consent must:
	+ be presented clearly, separately from other information, questions or permissions and in an accessible, plainly-worded format; and
	+ give a full explanation of how and for what purposes the Personal Data will be processed; and
* BU must able to show that the Data Subject has given consent. This means the individual should be asked to indicate consent by taking a positive action, such as providing a signature or ticking a box before submitting a form (often referred to as “opt-in” consent). It also means BU needs to keep records of the consent.

Arrangements to meet these requirements must be put in place before you proceed with any processing on the basis of consent.

* 1. In addition, individuals must be able to withdraw consent at any time; and BU must be able to respond to this by stopping the processing of the Personal Data. The ability to withdraw consent should, wherever possible, be made plain to the individuals at the time they give their consent.
	2. It is not appropriate to rely on consent as the condition of processing if withdrawal of consent would make it impossible to achieve the purposes behind the processing or would impede essential activities by BU. This will be the case for many core teaching, learning and research tasks within BU.
	3. If you intend to use consent as the basis for processing special category data, there is an additional requirement for that consent to be “explicit”. "Explicit consent" means that the consent must be absolutely clear and relate to the specific processing of the special category data: so it is particularly important to give details about how, why and by whom the processing will be undertaken. For evidential purposes, it is best practice (and BU's policy) to obtain all such consents in writing, i.e. through the individual signing a document which contains this explanation of the processing and a statement that they give consent to the processing.
1. **Sharing Personal Data with colleagues within bu**
	1. In accordance with the principle of data minimisation, Personal Data should only be accessed by, or made available to, those who have an appropriate authorisation from BU and a clear need to access the Personal Data for the purposes which form the legal basis of the processing. There is a significant risk that access by or disclosure to other persons (even within BU) will breach this policy and the Data Protection Legislation.
	2. Any decision to share Personal Data with additional people within BU or to increase access to Personal Data within BU should be made at an appropriate level and with clear consideration of the purpose and impact of the disclosure, the reasonable expectations of the Data Subject and whether there is a legal basis for the disclosure (taking advice from the Information Office or the DPO where appropriate). This principle applies irrespective of the seniority of the person(s) to whom the disclosure would be made or their relationship to the subject of the Personal Data. The PIA process should be followed where relevant.
	3. The fact that technically you can access Personal Data (e.g. the system does not prevent you opening a folder or file or a document has been left within your sight) does not mean that you should regard yourself as authorised to view or use that Personal Data: you should always ask yourself whether access is necessary and appropriate for the purposes of your role within BU.
2. **Disclosing Personal Data EXTERNALLY**

* 1. There are a number of established data sharing arrangements in place between BU and third parties, including partner organisations or contractors. These should be covered by a formal data sharing agreement or a contract which includes data sharing provisions, and should clearly allocate data protection responsibilities between BU and the other party.

You must act in accordance with these existing agreements and take advice from BU’s Information Office if any proposed disclosure is not covered by an existing data sharing agreement or where a new data sharing agreement may be required.

* 1. In any other circumstances, as a matter of policy, you should not disclose Personal Data externally without approval from BU's Information Office unless:
* the Data Subject has given clear consent to the disclosure (if the disclosure involves special category data, the consent must be recorded as required by section 12); or
* you are satisfied that the disclosure would be completely in line with the data subject’s reasonable expectations, e.g. as part of an established and transparent process, protocol or working arrangement.

You must seek advice if unsure whether either of these conditions is met.

* 1. There are circumstances when Personal Data can be disclosed without the individual's consent and even though the disclosure would not be anticipated by that individual. BU's Information Office will be able to confirm if any of the exemptions set out in the Data Protection Legislation apply to a proposed disclosure. You should always contact BU's Information Office (dpo@bournemouth.ac.uk or 01202 961315) if in doubt about whether a disclosure of Personal Data is permissible.
	2. For example, occasionally BU receives requests from external organisations, including the police and local authority fraud investigators, seeking Personal Data about Staff, External Members and students. BU may only disclose Personal Data to these organisations in exceptional circumstances after sufficient checks and conditions have been met. It should never be assumed that such organisations have the right to access or receive Personal Data. Such disclosures in relation to students should only be made in accordance with the [Guidance Note on Disclosure of Student Personal Data to Third Parties](http://intranetsp.bournemouth.ac.uk/policy/Guidance%20Note%20on%20Disclosure%20of%20Student%20Personal%20Data%20to%20%20Third%20Parties%20November%202014.docx). Similar considerations are required for any third party requests about Staff or BU Members.
1. **TransferS outside UK and those countries with an ‘adequacy decision’**
	1. You must not transfer Personal Data outside the UK and those countries, such as those in the European Economic Area (**EEA**), that benefit from an ‘adequacy decision’ without:
* the individual's explicit consent (where the individual has been informed of all the circumstances of the transfer); or
* confirmation from the Information Office that another justification exists under the Data Protection Legislation.

An adequacy decision is a regulatory decision that the legal framework in the relevant country has been assessed as providing ‘adequate’ protection for people’s rights and freedoms about their personal data. Further details of the current list of countries subject to an adequacy decision can be found on the ICO’s website. Notably, the USA does not presently enjoy an adequacy decision.

* 1. This applies even if the transfer is to a student living outside the UK or a country that benefits from an adequacy decision. In most cases this is unlikely to be a concern as the individual is likely to have already given their explicit consent; but unless it is clear their explicit permission has been given, for example in application forms, you must always check with BU's Information Office first.
	2. For routine and/or large-scale transfers of Personal Data around the world, for example to a third-party Data Processor engaged by a particular department, it will be necessary to put in place standard contractual clauses, and potentially take further investigatory and practical steps, to provide adequate safeguards for the Personal Data when it is transferred outside the UK or any country with the benefit of an adequacy decision. Again, please contact BU's Information Office in advance of any such international transfers of Personal Data being made.
1. **RETENTION AND DELETION OF PERSONAL DATA**
	1. Retaining Personal Data (even within archive) is a form of processing covered by the Data Protection Legislation. BU must only keep Personal Data for as long as is necessary for the purposes for which the Personal Data is processed. When new processing activities are developed and the legal basis for the processing identified, wherever possible a retention/destruction policy should also be established for that category of Personal Data. Where the purpose of retention is identified as being to meet legal or audit requirements, it is important to identify the specific requirement which applies.
	2. You must comply with relevant policies, processes or retention schedules which specify (or provide guidance on determining) the periods of time for which materials containing Personal Data should be retained and allocate responsibilities for reviewing and deleting/destroying records (links to some of these documents can be found [here](https://livebournemouthac.sharepoint.com/sites/DataProtection/SitePages/KB-Data-Retention.aspx) on the SharePoint site). You should also act in accordance with any information given to data subjects about the length of time for which their data will be retained. This means you must not retain materials after, or delete materials before, the end of a specified retention period unless you obtain specific, appropriate authorisation (e.g. from your manager or the DPO).

1. **data security**
	1. You must do all you can to ensure that Personal Data is not accessed or used without proper authority and is not lost or damaged. This will involve using all relevant data security tools which are made available by BU and generally using appropriate technical or organisational measures to protect the integrity and confidentiality of Personal Data and support data minimisation. It also means understanding, and taking reasonable steps to avoid, common methods of triggering cyber/data security attacks. You must complete all mandatory information security training requirements notified to you and comply with [BU’s information security policies](https://staffintranet.bournemouth.ac.uk/aboutbu/policiesprocedures/) (there is overlap in the content of those policies and this Data Protection policy). The steps you need to take will include for example:
* paper records which include Personal Data and in particular special category data must be kept securely in a cabinet or office which is locked when unattended;
* computers must be secured and locked when not in use;
* file encryption, anti-virus and security software, user passwords, audit trails and back-up systems must be securely used to protect Personal Data stored electronically;
* use of pseudonymisation or anonymisation tools should be considered, subject to technical or practical constraints;
* where Personal Data is being shared (either internally or externally) in accordance with this policy, appropriate protections must be applied to the Personal Data in transit (e.g. use of passwords, secure links or secure file transfer systems for electronic transmission, or use of recorded delivery or secure courier for hard copy transmission);
* you should be alert to cyber attack methods such as phishing and notify any suspicious contact to IT Services promptly in accordance with the information security policies and processes.
	1. You must not remove Personal Data from BU's premises unless:
* in the case of records held electronically, the Personal Data is stored in an encrypted form on a password protected computer or memory device; and
* in the case of hard copy records containing Personal Data, the records are stored securely and locked away at all times, including during transportation.
	1. You must not remove special category data from BU's premises without approval from BU’s Information Office.
	2. You must not use your own computer or own email accounts when processing Personal Data relating to BU if doing so would circumvent this policy. In particular you:
* should use remote access software and facilities provided and authorised by BU's IT Services when carrying out any BU related work;
* must not send BU related emails to your private email account(s);
* must not save files containing Personal Data onto your own computers and other personal devices; and
* must not leave devices unattended if they are being used (or could be used, without entering a password or some other access permissions) for BU related matters.
	1. You must not allow unauthorised access to BU computers or other computers containing BU related Personal Data. For example, you must not allow students or their friends and family access to work computers, folders containing work materials or work email account(s). Similar vigilance should be applied to Personal Data contained in paper files; such files should not be viewed in public (for example, on trains or other public transport), and they must never be left unattended, unless they have been appropriately secured (for example, stored in locked filing cabinets).
	2. Disposal of materials or assets containing Personal Data must be carried out securely, and in accordance with BU’s Asset Management Policy where this is relevant. Personal Data contained in hard copy documents must be placed in confidential waste bins so that those documents can be securely shredded before being disposed of appropriately. Where there is a requirement to delete Personal Data held electronically, or where IT assets are being disposed of, you must follow departmental procedures and seek support from IT Services as required to ensure that Personal Data is permanently deleted. Moving files into the recycle bin will not be sufficient to achieve permanent deletion.
1. **EXERCISE OF INDIVIDUAL RIGHTS UNDER THE DATA PROTECTION LEGISLATION**
	1. Individuals (including students, members of Staff and External Members and any other individuals whose Personal Data is processed by BU) have a number of rights under the Data Protection Legislation:
* request a copy of their Personal Data which is being processed by BU and information about that processing (a Subject Access Request). The information which must be provided about the processing includes the purposes of the processing, the length of time for which Personal Data will be kept by BU and details about any relevant third party data sharing;
* require BU to correct the Personal Data it holds about them if it is incorrect (**right of rectification**);
* to require BU to erase their Personal Data (**right of erasure/right to be forgotten**);
* to require BU to restrict its processing activities (and, where BU's processing is based on their consent, they may withdraw that consent to future processing) (**right to restriction of processing**);
* to receive from BU the Personal Data we hold about them which they have provided to BU, in a reasonable format specified by them, including for the purpose of transmitting that Personal Data to another Data Controller (**right to data portability**);
* to object, on grounds relating to their particular situation, to any of BU's particular processing activities where they feel this has a disproportionate impact on their rights (**right to object**).
	1. The above rights are not all absolute, and BU may be entitled to refuse or limit its response to such requests where exceptions apply. However, clear reasons must be given for any refusal, and there are tight timescales for responding to requests to exercise any of these rights.

As such, you must refer requests from individuals to exercise any of their rights under the Data Protection Legislation to BU's Information Office (dpo@bournemouth.ac.uk) **as soon as possible**. You should also promptly provide any assistance requested by the Information Office to help them respond to requests from individuals. This may include providing information about the way in which or the purposes for which Personal Data is processed by you/your department. You must not delete any materials covered by such a request after the request is received by BU, except with the authorisation of the DPO.

* 1. When generating materials which refer to an individual (e.g. file notes or emails relating to a student or a colleague) it is important to be aware that these materials will be the Personal Data of that individual. If they are retained in electronic form or filed in hard copy it is likely that they will have to be disclosed in response to a Subject Access Request.
1. For this policy, this comprises the UK GDPR and the Data Protection Act 2018. The UK GDPR is [Regulation (EU) 2016/679](https://www.legislation.gov.uk/id/eur/2016/0679), as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 as modified by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019. [↑](#footnote-ref-1)