LIVERPOOL HOPE UNIVERSITY
1844

LIVERPOOL HOPE UNIVERSITY
STAFF GUIDANCE ON DATA PROTECTION

www.hope.ac.uk

SUMMARY

The Data Protection Act 1998 (DPA) applies to the processing of personal data. Personal data is defined as data from which you can identify a living individual. From May 2018, the DPA will be replaced by the General Data Protection Regulation (GDPR). The core principles of data protection remain intact under the GDPR as do the majority of the main definitions. However, the GDPR is stricter about when we can use personal data, what we need to tell individuals about how we use personal data and how quickly we need to respond in the event of a personal data breach. The GDPR also requires us to demonstrate how we comply with the Regulation and introduce stricter fines for non-compliance.

The purpose of this guidance is to provide advice to staff on implementing procedures which support compliance with the law.

The law requires that we:

- Only use personal data where we need to and only use the minimum required to achieve our objectives;
- Are transparent about how and why we use personal data;
- Have a lawful basis for using that data;
- Have systems in place for correcting inaccurate personal data and keeping that data up to date;
- Have systems in place to securely destroy data where we no longer need it;
- Apply appropriate security measures which protect personal data; and
- Do not transfer personal data outside the EU unless very specific adequacy arrangements are in place.

The definition of personal data remains largely the same but has been slightly broadened under the GDPR to include reference to identifiers such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Sensitive personal data (known as special category data under the GDPR) is afforded a higher level of protection. Special category data is information about an individual's race, ethnicity, commission of a criminal offence (or the fact they have been subject to criminal proceedings), political opinions, religious beliefs and their membership of a trade union.

THE UNIVERSITY'S INFORMATION GOVERNANCE STRUCTURE

The University's Data Protection Policy sets out at a high level how the institution complies with data protection law. All staff are responsible for complying with the University's Data Protection Policy. At a managerial level, Heads of Departments and Managers are responsible for ensuring that staff follow the University's Data Protection policies, processes and guidance. In practice, this means Managers should make staff aware of such documents and, where appropriate, advise staff where those processes should be followed. The University's Senior Management Team similarly have responsibility for promoting these policies and processes at a senior level.

THE LEGAL PRINCIPLES OF DATA PROTECTION AND SOME PRACTICAL GUIDANCE

Principle 1: Personal data must be obtained and processed fairly and lawfully, and not processed unless certain conditions are met.

We can only process personal data if one of the lawful conditions applies.

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Special category data can only be processed if we can satisfy one of the conditions above and a further condition. These further conditions include:

- Explicit Consent from the data subject,
- It is necessary for fulfilment of a contract
- It is necessary for fulfilment of a legal obligation
- It is necessary to protect the vital interests of a person
- It is necessary for justice/public functions in the public interest
- It is necessary for legitimate interests

PRACTICAL GUIDELINES

Consent

Under the GDPR, valid consent can only be by active opt-in; as opt-outs, silence, inaction or lack of response are no longer valid. The University must be able to demonstrate (with evidence) that consent was given.

Where consent is given in a written declaration which also concerns other matters (e.g. a contract) the request for consent must be clearly distinguishable, intelligible and easily accessible. If this requirement is not complied with, the consent will not be binding; and

Data subjects need to be informed of their right to withdraw consent at any time and it must be as easy to withdraw consent as give it; and

Affirmative action to show consent can still be given by ticking a box or choosing appropriate technical settings. Silence and preticked boxes do not constitute consent. Where consent is relied on for the purposes of processing sensitive personal data, consent must be explicit. As the requirement for consent is now so high, the line between what constitutes consent and what constitutes explicit consent becomes ever more blurred. We await further guidance on what, if any, distinction there is.

You should contact The Head of Legal Services, Governance and Risk if you cannot determine whether or not a condition for processing.

Privacy Notices

In the context of the first principle, fairness means transparency. The University must communicate to data subjects, in a privacy notice, what data it will collect and process, the legal basis of the processing, the purpose of the processing, who the University will share it with and how long it will be retained. The notice should also include information about access and other rights over the data (including the right to lodge a complaint with a supervisory authority), details of any transfers outside of the EEA and safeguards applied to such transfers, as well as contact details of the data controller's data protection officer

We may need to create privacy notices for each University service.

In most cases, the University will have provided this information to students in the Student Fair Processing Notice. If your reason for using students' personal data isn't addressed in the fair processing notice for students then contact the Head of Legal Services who can arrange for the notice to be updated or advise on alternative methods for communication.

If you need to provide the fair processing notice for a very specific service or purpose (such as an online survey or a recruitment site), please contact the Head of Legal Services, Governance and Risk who can provide you with a template notice.

Principle 2: Personal data must be obtained for specified and lawful purposes and not processed in any manner incompatible with those purposes.

This means that, once we have collected and are holding personal data, we cannot then use the data for another activity or for any reason the data subject would not expect or did not originally agree to.

Any use of personal data should be checked against what the data subject was originally told and the consent previously provided. Any additional or re-use of the data collected for some other purpose will normally require obtaining new consent from the data subject.

This principle is of particular relevance to staff involved in research or marketing activities. Just because the University holds data about lots of students, it does not mean we can then use that data to conduct research, or use/share that information for advertising purposes, without notifying or obtaining the data subject's consent.

PRACTICAL GUIDELINES

Consider whether you need personal data to achieve your objective.

Only collect or use the minimum amount of personal data needed for your specific business objective.

For example, to administer a car-parking scheme, a University team may need to collect an individual's name, car registration number and University ID number but would not need to collect other types of personal data such as age or ethnicity to administer that scheme.

Principle 3: Personal data must be adequate, relevant and not excessive for the purpose.

We must collect sufficient information for the intended purpose; insufficient data may be a breach under Principle 3, for example, destroying a student's marks or feedback before an Exam Board or before the deadline for submitting an appeal. However, too much information may also be a breach – anything that isn't required is an unnecessary invasion of privacy.

Collecting or recording information 'in case' it might be useful is not permitted. Beware of recording or sharing opinions or excessive details stick to factual information. This principle is also important when designing forms/questionnaires, stick to what is relevant and necessary.

The GDPR emphasises data minimisation (collecting and using the minimum data necessary to fulfil the purpose) and privacy by design (determining at the outset the data required for the purpose).

Principle 4: Personal data must be accurate and kept up to date.

Always use central sources of data where possible – these are most likely to be up to date and accurate. Avoid creating unnecessary copies of data (such as your own list of contacts) which will quickly become out of date and inaccurate. Act promptly to ensure that records are updated quickly when there is any change in staff/student circumstances or data. Ensure records are checked and updated regularly. Follow the University's record management policy and schedule. Regularly destroy out of date information and data which is no longer required.

Mistakes in this area are easy to make, but can have serious consequences: Failing to update an address quickly or accurately can result in a disclosure of data to the wrong person. Simple procedures and good practice can prevent a breach.

Where possible Departments should implement processes which enable individuals to update their personal data where they need to update information such as a change in address.

Departments should be clear on individual staff members' responsibility for updating personal data where data is inaccurate or out of date.

Principle 5: Personal data must not be kept for longer than is necessary for the purpose.

Effective records management is vital for data protection compliance.

You should not store information indefinitely, keeping data for too long is a breach of Principle 5. Regularly review, archive and delete older data. Information no longer needed or out of date should be safely destroyed/deleted.

Records management applies not just to paper files/documents but to electronic records and emails.

Paper and electronic files and emails should be tidy and well organised. You should know what data you are holding and where to find it, quickly, when required. Instructions on how to dispose of confidential waste (including items such as CDs/DVDs) are available on the University website under the Information Management Policy. For instructions on how to dispose of IT equipment, contact IT Services.

Departments will need to keep a record of the retention periods for the personal data they process in their teams. Some retention periods are set out in the Information Management Policy.

Heads of Department/Managers should make clear to their staff who have responsibility for destroying particular records when the retention period for those records has expired. Heads of Department/Managers should ask staff to report on a regular basis to confirm records have been destroyed within these periods.

Personal data must be destroyed in a suitably secure manner. Personal data in records should be disposed of in the University's marked confidential waste bins. Staff should never dispose of personal data in regular waste bins.

Advice on how to delete email and other electronic records can be obtained by contacting IT Services.

When procuring new IT systems, consideration is needed as to whether the system can be designed to delete records after a particular retention period has expired. Where teams are procuring IT systems which are used to process personal data then the Head of Department/Manager should ensure that a Data Protection Impact Assessment is undertaken. This will help identify functional requirements (such as automatic deletion) which can help support Data Protection compliance.

Principle 6: Personal data must be processed in accordance with the data subject's rights under the Act.

Below are the main rights that people have in relation to their personal data:

- know why their data is being collected
- what it will be used for
- how long it will be kept for
- know who the University will share their data with
- ask for access to the data that the University holds about them
- give permission for their data to be held/processed
- to opt out of unnecessary processing
- object to data processing that causes damage or distress

There is also a new right to prevent Profiling. Profiling is any form of automated processing of personal data to analyse or predict aspects concerning an individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. The GDPR prohibits data controllers from subjecting a data subject to a decision based solely on automated processing of sensitive data, except in limited circumstances. This could be problematic for researchers and analytics teams working in this space. In circumstances where profiling is permitted, the data controller must implement suitable measures to safeguard the data subject's rights and interests. Additionally, a data controller who uses profiling techniques must implement appropriate technical and organisational measures to safeguard against inaccuracies and prevent discrimination. The data subject should be informed in the privacy notice of the existence of profiling, the logic used and the significance and likely consequences of such profiling.

If you receive a request from an individual to exercise any of the above rights, then you will need to inform the Head of Legal Services, Governance and Risk as soon as possible, who will advise on and help co-ordinate the University's response to such requests. There are strict timescales for complying with the above rights (one month in some cases) so please do not delay in getting in contact.

▶ Sharing of Personal Data

Internal Sharing Guidelines

Only share personal data with other teams/departments where those teams have a genuine business need to access the personal data.

Only share the minimum amount of personal data those teams need to deliver their business objective. If you plan to share personal data with a department on a routine basis and haven't previously done so, inform your Head of Department or Manager of the proposal. If you or your Head of Department or Manager have concerns about sharing the personal data then contact Head of Legal Services, Governance and Risk for advice.

Departments should consider implementing a secure method of sharing the personal data between your teams.

For example, if you need to share large volumes of data or sensitive personal data on a regular basis with another team you could establish a shared folder on the University's own systems. You would need to limit the access to the appropriate individuals.

Alternatively, you could apply the password protect feature to the spreadsheet containing the personal data. The password should be sent separately from the spreadsheet.

If you are the team receiving the personal data, you will need to consider whether individuals have been informed about the intended use of the data.

If you are using the data for an entirely new purpose, you may need to undertake a Data Protection Impact Assessment (DPIA). Seek guidance from the Head of Legal Services, Governance and Risk.

External Sharing Guidelines

You may receive a broad range of requests from external organisations to disclose personal data. You should only disclose personal data to external organisation where they have the individual's consent to do so or where there is another legal basis for doing so.

For example, you may receive a request from the police asking for information about a student in the context of a criminal investigation. If you receive such a request please contact Company Secretary, Proctor and Head of Committees who will review the request to ensure there is a lawful basis for disclosure and will make the disclosure to the police if deemed appropriate.

If you are satisfied that you have an individual's consent to disclose or there is another alternative legal basis to make the disclosure, then before you disclose the personal data make sure you are confident about the requester's identity.

If you are contracting an external organisation to deliver services on behalf of the University you will need to enter into a contract with that organisation which imposes specific measures such as requiring the contractor to impose appropriate security measures to protect the data. Please contact the Head of Legal Services, Governance and Risk for advice on putting in place a contract.

If you are sharing personal data on a regular basis with another organisation and you aren't paying that organisation for a service then it may be necessary to enter into an information sharing agreement. In particular, an information sharing agreement should be in place if sharing high volume data or data of a particular sensitivity (such as medical information or information about criminal offences).

Each department/team should maintain a central list of organisations with whom they regularly share personal data including contractors, other Universities, government bodies and other public authorities etc. Departments should regularly review these lists to assess whether you are sharing with new organisations or whether your existing contracts or agreements with these organisations need to be updated.

Principle 7: Personal data must be kept safe from unauthorised access and processing, and from accidental loss, damage or destruction.

Breaches of Principle 7 are the most common cause of fines issued by the ICO, usually as a result of a simple error by an individual. Due to the potential for serious harm as a result of a breach in data security, the Information Commissioner has even imposed fines on organisations even where a breach caused no unauthorised disclosure or actual harm to the data subject.

PRACTICAL GUIDELINES

Verify the identity of data subjects before you release any information to them. The exact method of identity check will vary, depending upon whether the individual is current or former staff/student and the nature of the situation. Set a departmental protocol for identity checks, especially if you regularly disclose information to staff/students.

Implement departmental controls to restrict access to systems/documents containing personal data, so that only those staff who are authorised and need to view the data for specific work purposes can do so. Personal data should not be available to all staff at all times, just in case it might be useful. Information should be available and shared on a need to know basis only.

Use the secure areas provided (or approved by) the University for working on and storing personal data such as encrypted devices and network drives. Software and cloud storage solutions which are not approved by the University are a risk as they may store information on servers outside the EEA, which may breach Principle 8. Do not download or store any data on non-encrypted computers/devices.

If you intend to use a cloud-based system to store personal data, then you must check that the contract with the provider has been reviewed by Head of Legal Services, Governance and Risk and the security controls for that system have been reviewed by IT Services. If you are unsure whether a system you currently use has been assessed then please contact IT Services who can help provide a risk assessment and options for strengthening security where appropriate.

Simple Steps to Compliance

- Keep documents and screens out of sight of others.
- Position computer screens so that they cannot be viewed by an unauthorised person from a window or glass partition behind you.
- Lock doors and filing cabinets. Information left unattended is more likely to be stolen, disposed of in error or disclosed to the wrong person.
- Clear your desk! Tidy confidential data away when it is not being used.
- Papers containing personal data should not be taken out of the University.
- Anonymising data makes it safe. Pseudonymising data also reduces risk.
- Only store personal data on Liverpool Hope University approved systems.

Emails

- Emails require particular care. In general, email is not a secure method for transmitting personal data – use these checks to avoid a breach:
- Does it contain personal data?
- Is it ok to email?
- Remove unnecessary content and attachments.
- Avoid forwarding entire emails, 'email trails', and attachments, unless you have checked it for personal data and it is necessary for recipients to see.
- Sensitive content can be sent in an encrypted attachment (password protected word or pdf document) with the password provided separately.
- Beware of the autocomplete function which can easily result in emails being sent to the wrong recipient.
- Do you have the sender's permission to forward or share their name/email address? You should always use the bcc (blind-copy) function so the recipients can't identify each other:

Principle 8: Personal data must not be transferred to a country outside the EEA, unless that country has equivalent levels of protection for personal data.

As Data Controller, the University is responsible for protecting personal data which is sent, transferred to, or stored in non-EEA countries. The GDPR prohibits the transfer of data outside of the EU other than in compliance with the conditions for transfer set out in Chapter V of the GDPR. It will be possible to share personal data in jurisdictions that do not have adequate protection only if there is a legitimate basis, it is not a repetitive exchange, involves a limited number of data subjects, the data subjects are informed of the transfer and the relevant supervisory authority (the ICO) is informed. This means we will need to carefully think about the data we share with our international partners.

Contractual clauses may also be needed to ensure protection in countries where there is no Data Protection Act (or equivalent) in place. If your project is doing business with a company outside the EEA, you must ensure the Data Protection clauses in the contract are approved by the Head of Legal Services, Governance and Risk. Many types of software and mobile app providers are not UK based and they store information outside the EEA, via the cloud. You should only use the University's approved methods of data sharing and storage.

PERSONAL DATA BREACHES

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Data means information in any form; paper records, emails, faxes etc. Examples of personal data breaches can include forwarding a spreadsheet of student data to an unintended recipient (external or internal) or a theft of sensitive documents left in an unlocked room or leaving a laptop unattended somewhere. **Personal data breaches must be reported to the Head of Legal Services, Governance and Risk immediately.**

You will need to provide details about the circumstances of the breach, the type of data involved and who that data relates to and potential impact on individuals affected.

The University will be subject to a strict 72 hour timescale in which to report such breaches to the regulator, the Information Commissioner. The University can be fined for failure to report within the period. The 72 hour timeframe starts from the moment **any** individual in the organisation (not just Legal) discovers that a personal data breach has occurred.

If the breach occurs out of hours or during shut down periods you should contact the Security Lodge at Hope Park who has emergency contact details for the relevant management team members.

Laura Gittins

Head of Legal Services, Governance and Risk (February 2018)
T: 0151 291 3478
E: gittinl@hope.ac.uk

FOR MORE INFORMATION PLEASE CONTACT

Laura Gittins

Liverpool Hope University
Head of Legal Services, Governance and Risk (February 2018)
Liverpool
L16 9JD

T: +44 (0)151 291 3478

E: gittinl@hope.ac.uk

www.hope.ac.uk

LIVERPOOL
HOPE
UNIVERSITY
1844

TEF
Gold