

WORKING WITH THE POLICE AND OTHER LAW ENFORCEMENT AGENCIES

Request for Disclosure of Personal Data (subject access requests)
Under section 29(3) of the Data Protection Act 1998 and GDPR

Guidance & Procedures

Issue:	2	Prepared by:	Authorised by:
Date:	May 2015	Equality, Inclusion and Safeguarding Advisor	Principal.
Reviewed:	April 2018		Approved by:
Next Review:	April 2020	2 Years	Corporation

Glossary of Terms:

Anonymised Data - This is data which does not identify an individual directly, and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full postcode and any other detail or combination of details that might support identification.

Data - Within this guidance data could include personal and/or sensitive personal data

Data Subject – The individual person who is the subject of the data request. In this Policy, the data subject will be referred to as the 'individual'.

Disclosure - This is the divulging or provision of access to data.

Explicit Consent - This means an articulated agreement and relates to a clear and voluntary indication of preference of choice. This will usually be given freely, either orally or in writing and freely given in circumstances where the available options and the consequences have been made clear.

Implied Consent - This means an agreement which has been signalled by the behaviour of an individual, with whom a discussion has been held regarding the issues and whom therefore understands the implications of the disclosure of data.

Interagency Information Sharing Protocol Information Sharing Protocol (v.8 February 2015) -

The protocol refers to high level document setting out the general reasons and principles for sharing data. The protocol will show that all signatory organisations are committed to maintaining agreed standards on handling data and will publish a list of senior signatories. It should be underpinned by data sharing agreements between the organisations who are actually sharing the data.

Information Sharing Agreement - This agreement is a more detailed document the intention of which is to spell out how the organisations involved will operate their approach to data sharing. Agreements will be produced whereby organisation specifically identifies a purpose to share data across organisational boundaries. The agreement should state whether partners are obliged to, or are merely enabled to, share data.

PCD- Personal Confidential Data - "Personal confidential data" is defined in the Caldicott 2 Report as *"Personal information about identified or identifiable individuals, which should be kept private or secret"*. It also includes information about the deceased.

Pseudonymisation - Pseudonymisation is a procedure whereby the most identifying fields within a data record are replaced by one or more artificial identifiers. There can be a single pseudonym for a collection of replaced fields or a pseudonym per replaced field

Relevant Legislation:	
<input type="checkbox"/> Access to Health Records 1990	<input type="checkbox"/> Education Act 2002
<input type="checkbox"/> Data Protection Act 1998	<input type="checkbox"/> Mental Capacity Act 2005
<input type="checkbox"/> GDPR	<input type="checkbox"/> Local Government Act 2000
<input type="checkbox"/> Crime and Disorder Act 1998	<input type="checkbox"/> Homelessness Act 2002
<input type="checkbox"/> Human Rights Act 1998	<input type="checkbox"/> Safeguarding Vulnerable Groups Act 2006
<input type="checkbox"/> Freedom of Information Act 2000	<input type="checkbox"/> Criminal Justice Act 2003
<input type="checkbox"/> The Children Act 2004	<input type="checkbox"/> Civil Contingencies Act 2004
<input type="checkbox"/> Mental Health Act 1983	<input type="checkbox"/> Health and Social Care Act 2012
<input type="checkbox"/> Common Law Duty of Confidentiality	

1. Introduction

The College is committed to all aspects of data protection and takes seriously its duties under the Data Protection Act [DPA 1998] and GDPR. This policy will apply to all requests for information concerning staff, students and any individuals who are providing services on behalf of the College.

Working with the Police and other law enforcement agencies is vital for ensuring the detection and prevention of crime. Therefore, sharing data with the Police / other law enforcement and assisting them with their enquiries is essential for the purposes of law enforcement and public protection.

The College also recognises that individuals also have specific rights in relation to their personal information being held by the College. The College will also balance the rights of the individual and always aim to share 'person-identifiable confidential data' with the individual's express consent, unless a legal or statutory requirement applies for the disclosure to be made without the express consent of the individual.

The College understands the following risks associated with the disclosure of sensitive information:

- Mishandling data can cause harm and distress to families and children, and put them at risk
- Complaints or possible court action by affected individuals
- Damage to an organisation's reputation, including loss of trust by members of the public
- Enforcement action by the Information Commissioner's Office which can include fines of up to £500,000 for serious breaches of the Data Protection Act.
- Comply with the GDPR

This guidance and the associated procedures outline the general protocols for working with the Police and other law enforcement agencies at Leeds College of Building. It explains the principles the College needs to consider, when asked to release personal and sensitive information relating to an individual, whether this is with the consent of the individual or in a situation, or where information is disclosed without an individual's explicit consent. The guidance will be in line with the College's responsibility to handle, process and store data responsibly in compliance with the eight data principles in the Data Protection Act [1998] and GDPR,

The following staff at Leeds College of Building have authority to make a decision on whether or not to release the personal information. They will be briefed on their responsibilities on this procedure.

Authorised staff include;

- Members of the Senior Management Team,
- Assistant Faculty Directors
- Equality, Inclusion and Safeguarding Manager
- Student Services Manager.
- Neil Kline (only CCTV requests)

2. Police Requests for Personal information

2.1 The Police, and other authorised agencies, may request personal data about specific individual(s) from the College for the purposes of:

- the prevention or detection of crime,
- the apprehension or prosecution of offenders,
- in emergency situations.

Examples of the type of information which could be requested is below:

Type of data	What is it?	Examples
Personal data	Data that relates to a living person. This may include: <ul style="list-style-type: none"> • Names of staff and pupils • Date of birth • Addresses • National insurance numbers 	<ul style="list-style-type: none"> • Staff development reviews • School marks and exam results • Attendance reports
Sensitive personal data	Sensitive personal data needs to be treated with more care. It includes details about: <ul style="list-style-type: none"> • Race and ethnicity, disability or learning difficulty. • Political opinions • Religious beliefs or membership of trade unions • Physical or mental health/medical information • Sexuality • Criminal offences, including alleged offenses • Child protection and safeguarding disclosures • Abuse and neglect of children and adults 	<ul style="list-style-type: none"> • Special Education Needs (SEN) / (EHCP's) assessments • Occupational health reports • Case notes • Social care documents • Disclosures of abuse • Disclosures of criminal activity
Sensitive commercial data	Data which relates to a commercial contract that could result in a breach of contract or financial loss if disclosed in error.	<ul style="list-style-type: none"> • A document that includes contractor rates • Information relating to contract negotiation and performance

2.2 Section 29 of the DPA provides authorised agencies with the mechanism to request, and the College the authority to either release or decline to release, personal data without the explicit consent of the individual(s).

2.3 The DPA allows the release of personal data about an individual in an emergency (e.g. for medical, accident and next-of-kin situations), in order to protect the vital interests of that individual or another individual.

2.4 Section 29 of the DPA allows the College to disclose personal data on specific individual(s) to the Police, or other authorised agencies, if the College is convinced that failure to disclose the information would prejudice a Police investigation (please note, disclosure is at the College's discretion).

2.5 The Data Protection Act includes exemptions which allow personal data to be disclosed to law enforcement agencies without the consent of the individual who is the subject of the data, and regardless of the purpose for which the data originally gathered. In particular, personal data may be released if:

- The information is required for safeguarding national security (Data Protection Act section 28); or
- Failure to provide the data prejudice the prevention or detection of crime, the apprehension or prosecution of offenders,
- or the assessment or collection of any tax or duty (Data Protection Act section 29(4)).

3. Dealing with request for personal information from the Police and other law enforcement agencies.

3.1 Police forces have standard forms (known as section 28/section 29 forms) for requesting personal data, in accordance with guidance issued by the Association of Chief Police Officers (ACPO). The form should state that:

- any information is required for an investigation concerning national security, or
- the prevention or detection of crime, or the apprehension or prosecution of offenders,
- any investigation would be prejudiced by a failure to disclose the information.

This provides the College with a legal basis for supplying data under the exemptions in the Data Protection Act. All requests for personal data from the police, apart from emergency requests, should be required to be on a 'Section 28/ 29(3)' form. The completed form will briefly outline:

1. the nature of the investigation and the reason that information is required,
2. the individual(s) about whom the Police require data,
3. the individual(s) role in that investigation,
4. the information required about the individual(s),
5. the name and number of both the requesting and authorising Police Officers.

3.2 Other law enforcement agencies may not use standard forms.

- All other law enforcement agencies will be asked to complete a 'S29Request Form' and return it to the designated persons at the College.
- If a properly completed form is received, the data should normally be disclosed.
- However, the College may decline to provide the information for the reasons detailed below in 3.3.

3.3 The grounds on which the College may decline to release the requested personal information

If the College has genuine concerns about releasing the personal information, and believes that the processing / disclosure of personal information about an individual is causing, or is likely to cause, substantial and unwarranted damage or distress to the individual(s), the College may refuse to provide the information and ask the Police or other law enforcement agencies to come back with a court order requiring the College to release that information.

The authorised member of staff should ask themselves the following questions when considering a request for information.

“The College may refuse the section 28 / 29(3) request from the Police because;

- *the College has other relevant legal obligations*
- *the disclosure of the information may conflict against the legitimate rights of others,*
- *someone’s safety may be put at risk by releasing the information.”*

If a court order is obtained, then the College will either obey that order, or may ask for the order to be varied or revoked because;

- a) there has been a material change of circumstances since the order was made, or
- b) the facts on which the original decision was made were (innocently or otherwise) misstated.

4.0 Emergency requests

4.1 Schedule III(3) of the DPA allows the release of personal data about an individual in an emergency, e.g. for medical, accident or next-of-kin situations etc in order to protect the vital interests of that individual or another individual.

4.2 An emergency situation is one where the College has reasons to believe that there is a danger of death or injury to a member of the College Community or any other person. The police and other emergency services may urgently require personal data from the College, and may not have time to

complete a formal written request. In these circumstances, data can be legally disclosed provided it has been authorised by one of the following persons;

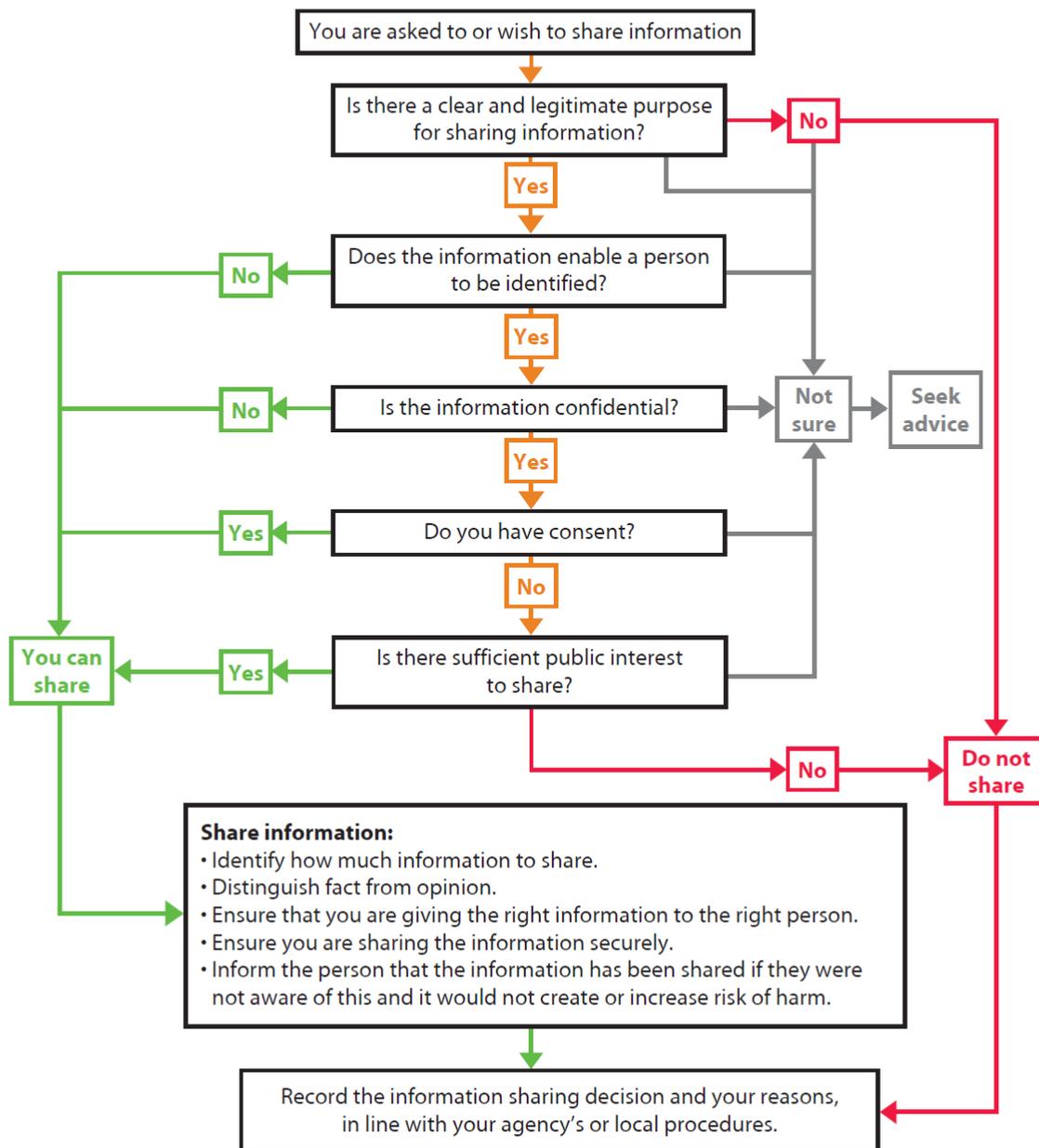
- Senior Management Team,
- Equality, Inclusion and Safeguarding Advisor
- Student Services Manager.
- Assistant Faculty Directors
- Neil Kline (only CCTV requests)

The request should be followed up by a formal written request as soon as possible.

5.0 Procedures when a S29 request is received.

Step 1
<p>One of the following authorised persons will ensure the correct form is received;</p> <ul style="list-style-type: none"> • A member of the Senior Management Team, • Equality, Inclusion and Safeguarding Manger • Student Services Manager. • Neil Kline (<i>only CCTV requests</i>) • Assistant Faculty Directors
Step 2
<p>For all cases, including those refused, the request must be logged on S29 REQUEST FORM (or attached to) for audit purposes which must include;</p> <ul style="list-style-type: none"> • details of the request • an assessment of the veracity of the request, • the requestor(s) name and role [eg: Police Officer, Immigration Officer, Tax Authority], • the requestor(s) warrant card number or similar official identification details - when appropriate • the College person(s) handling the request, • the action(s) taken, • the date/time for each action, • the information released and how it was released [email, by post or other media formats] <p>The request forms will be stored in the Safeguarding Case Files folder G:// under 'Section 29(3) Requests' with limited access to authorised persons.</p>
Step 3
<p>Ensure that all requests for information are received in writing from the relevant authority on the correct form (i.e a section 29(3) form from the Police). A request by phone is not generally acceptable but the College may accept a faxed or email form.</p>
Step 4
<p>If a properly completed form is received, the data should normally be disclosed if the authorised person is satisfied that the request meets one or more of the requirements outlined in section 2 or 4 of this guidance. The response to this request should be signed off by the authorised member of staff. (<i>for emergency requests for information, the guidance in section 4.0 should be followed</i>).</p>
Step 5
<p>Copies of the form used to request personal data, other correspondence with the law enforcement agency and a copy of any data released should be retained by the College for <u>6 years</u>.</p>

Flowchart of key questions for information sharing



If there are concerns that a child may be at risk of significant harm or an adult may be at risk of serious harm, then follow the relevant procedures without delay.
Seek advice if you are not sure what to do at any stage and ensure that the outcome of the discussion is recorded.

S29 Request Form

Request For Disclosure Of Personal Data - Under section 29(3) of the Data Protection Act 1998

All requests must be submitted via email to S29Requests@lcb.ac.uk or fax to: 0113 2226001

<p>Section 1.</p> <ul style="list-style-type: none"> ■ Please provide your name, job title and organisation to enable us to identify you as a person with statutory authority to make a request under the exemption. ■ Please include the address, a secure email address and a telephone number to allow us to contact you or forward the information once a decision has been made. ■ Please include your fax number if you require the requested information via facsimile 	
Requested by (Name)	
Job Title	
Organisation & Address	
Email	
Telephone number	
<p>Section 2</p> <ul style="list-style-type: none"> ■ Please specify the information you are looking for and, where known, any other details which would enable us to locate the data e.g. directorate or section the individual has had contact with, where the data is likely to be held or the dates when the individual was in contact with the College. ■ You can attach any additional documents which may help us to locate the information, or identify the data subject. Please tick the attachments box where indicated if you are sending any additional information. ■ For the purposes of crime prevention or apprehension/conviction of an offender the requested information should relate to a specific individual. This exemption must not be used for 'trawling' information and these requests will be refused 	
Name	
Address	
Other identifying information	
Specific information required	
Attachments	Yes <input type="checkbox"/> No <input type="checkbox"/>
<p>Section 3</p> <ul style="list-style-type: none"> ■ Please supply details of the offence. Where you are unable to specify the offence please tick the appropriate box. This should only be used where it is likely to prejudice the case as this information can aid the decision making process. ■ Please give reason(s) why the information is necessary. ■ Please also state under what powers you are requesting the information. <p><i>The College reserves the right to withhold data if sufficient grounds for applying an exemption are not provided.</i></p>	
Offence	<i>Unable to specify offence due to risk of prejudice to case</i> <input type="checkbox"/>
Reason why information is necessary	
State under which statutory powers you are requesting the information	
<p>I certify that the data is required for one of the following purposes (please tick appropriate one), and non-disclosure would prejudice that purpose. I also certify that it will not be used in any way incompatible with the purpose: -</p> <p> <input type="checkbox"/> the prevention or detection of crime, <input type="checkbox"/> the apprehension or prosecution of offenders, <input type="checkbox"/> in emergency situations. <input type="checkbox"/> collection of tax, duty or imposition of similar nature </p>	
<p>Section 4: Disclosure</p> <p><i>The College reserves the right to withhold data if sufficient grounds for applying an exemption are not provided.</i></p> <ul style="list-style-type: none"> ■ Please state how you would like to receive the information. ■ If you wish to collect the information then we will require sufficient identification for example an ID badge or a warrant card. ■ Please indicate the timescale in which you require the information. Dependent on number received, volume and nature of request it may take up to 5 days to process. ■ When we receive a completed section 29 form we will assess whether or not this information will be released. We will endeavour to provide the information you have requested as soon as possible and will inform you if it is not possible to meet the required timescale. 	
How would you like to receive the information?	
email – please provide address	
Post:	
fax numbers will be accepted in exceptional circumstances	
Collection	
Please indicate the date by which the information is required:	

Section 5 Authorisation

- Once you have completed your form please submit as appropriate. Please include the email address of the authorising officer as confirmation.
- For requests from the Police, the form must also be authorised by a person no lower than Police Inspector. If the College does not consider the level of authorisation signatory to be sufficient we reserve the right to request further authorisation or to refuse to supply the information.

Failure to complete the form fully is likely to delay the process of obtaining the information.

Please note that the final decision to release the requested information is held by the College.

- I understand that if any of the information given on this form is incorrect, I may be committing an offence under section 55 of the 1998 Data Protection Act.
- The authorisation email acts as authentication and must be in the recognised police/government formats (i.e. - email addresses containing .gsi or .gsx or .pnn). In certain circumstances we may ask for further details to confirm authentication.

Name of officer/requestor [Block Capitals]	
Authorising officer/requestor Email address	
Job title of authorising officer/requestor	
Date	

For official use only

1. For which purpose if the data required?	<input type="checkbox"/> the prevention or detection of crime, <input type="checkbox"/> the apprehension or prosecution of offenders, <input type="checkbox"/> in emergency situations. <input type="checkbox"/> collection of tax, duty or imposition of similar nature
2. Is this request a genuine and necessary? (are there other ways to obtain the information?)	<input type="checkbox"/> Yes <input type="checkbox"/> No Please include any other relevant information:
3. Requestor(s) name and role [eg: Police Officer, Immigration Officer, Tax Authority],	
4. the requestor(s) warrant card number or similar official identification details - when appropriate	
5. The College person(s) handling the request,	
6. the action(s) taken,	<input type="checkbox"/> Approved <input type="checkbox"/> Declined <input type="checkbox"/> Declined and asked to obtain a court order If approved, what information was released? If the request has been declined, please state the reason for this below:
7. How has the information been released?	<input type="checkbox"/> email, <input type="checkbox"/> by post <input type="checkbox"/> Fax <input type="checkbox"/> Collection in person
8. The date/time	

All requests must be submitted via email to S29Requests@lcb.ac.uk or fax to: 0113 2226001