大连理工大学学校办公室文件

大工办发〔2019〕51号

关于印发《大连理工大学信息化个人信息保护管理办法（试行）》的通知

校内各单位、机关各部门:

为规范学校信息化建设中个人信息的处置，明确信息化建设中对个人信息保护的管理要求，避免个人信息处置不当造成师生、学校及其他相关部门、人员利益受损,按照《中华人民共和国网络安全法》、《中华人民共和国刑法》等法律法规要求，根据国标《GB/T35273-2017信息安全技术个人信息安全规范》及公安部《互联网个人信息保护指南》意见，特制定本办法。经2019年6月26日校长办公会审定通过，现予以印发，请遵照执行。

附件:《大连理工大学信息化个人信息保护管理办法(试行)》

2019年7月4日

学校办公室秘书科　　2019年7月4日印发

附件：

大连理工大学信息化个人信息保护管理办法（试行）

第一章 总则

第一条 为规范学校信息化建设中个人信息的处置，明确信息化建设中对个人信息保护的管理要求，避免个人信息处置不当造成师生、学校及其他相关部门、人员利益受损,按照《中华人民共和国网络安全法》、《中华人民共和国刑法》等法律法规要求，根据国标《GB/T35273-2017 信息安全技术个人信息安全规范》及公安部《互联网个人信息保护指南》意见，特制定本办法。

第二条 本办法适用于学校信息化建设中所涉及的个人信息采集、存储、使用、共享、公开及删除等各环节。在学校信息化建设中，为满足学校教学、科研及校务管理需求，且符合国家及相关主管部门在学籍、教务、人事、财务、档案、设备、资产管理等方面的法律法规及规章制度要求时，可依照本办法处置校内师生的个人信息，校内师生有义务提供相关个人信息。

第三条 根据国家法律法规和国家标准，本办法中个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，包括但不限于如下信息:

姓名、出生日期、身份证件号码、个人生物识别信息、银行

账号、住址、个人通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、成绩信息等。

个人敏感信息指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息，包括但不限于如下信息:

身份证件号码、个人生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14 岁以下（含）儿童的个人信息等。

第四条 在学校信息化建设中,个人信息保护应遵循如下原则:

1. 合法原则：不得违反相关法律、法规的规定;

2. 最小必要原则：在满足信息化建设必要需求前提下，在最小范围内采集、存储、使用个人信息，对于个人信息的处理采用最小操作权限划分，不得超范围处置个人信息;

3. 安全原则：信息化建设中应采用必要的安全技术措施和管理手段，保障个人信息的完整性、保密性及安全性，避免个人信息泄露、损毁和丢失;

4. 知情同意原则：学校对在科研、教学及校务管理中使用到的个人信息，依法依规进行采集和使用；其他信息化应用中使用的个人信息，应明确告知相关个人，并由个人自愿同意后，方可使用。

第二章 责任分工

第五条 学校信息化建设中个人信息保护工作由学校网络安全与信息化管理委员会下设的网络与信息安全工作组负责领导，由网络与信息化中心（以下简称网信中心）负责组织实施、监督检查，各信息化数据的主管部门负责具体落实本部门管理的个人信息的安全保护工作。

第六条 校内师生为其个人信息所有者，在学校信息化建设中，师生有权查询本人的个人信息，有权更正错误的个人信息，有权对信息化建设中违规处置个人信息的行为进行反馈和报告。对于各信息化项目中的违规行为可以向项目主管部门反馈，主管部门应予以及时处理并反馈处理结果。

第七条 校内师生作为个人信息的所有者，有义务及时更新信息化建设中使用到的个人信息，保证信息的准确性和完整性，并在信息化应用过程中妥善保管个人信息。由于师生个人原因造成的个人信息泄露、损坏、丢失，由本人承担相应责任；如对他人个人信息造成不良影响，将根据本办法的追责条款，追究相关责任人的责任。

第三章 个人信息的采集、存储、使用、共享、公开与删除

第八条 学校信息化建设中的个人信息采集，统一由相关数据的主管部门负责，个人信息主管部门由《大连理工大学信息化数据资源管理办法》相关规定确定。数据主管部门原则上必须把相

关业务系统作为数据源系统，不允许线下采集，其他业务部门、信息化项目不允许单独进行个人信息采集。个人信息主管部门应对采集的个人信息进行审核和及时更新，确保个人信息的准确性和完整性。师生个人信息如发生变更或采集的数据有误，可向该信息主管部门提出更新申请，主管部门应提供方便、快捷的信息更新渠道，保证及时更新个人信息。

对于未纳入业务部门管理的个人信息数据，由学校公共数据平台进行采集，师生可随时在公共数据平台中对未纳入部门管理和不需要部门审核的个人信息数据进行维护。

第九条 在学校信息化建设中，学校公共数据平台是个人信息集中统一的存储平台。个人信息主管部门采集到的个人信息，除存储在相关的业务系统数据库中，还应通过学校相关数据交换途径，交换到学校公共数据平台中。

个人信息在存储和传输过程中必须进行加密处理，采取有效技术手段和管理措施保护存储个人信息的服务器和数据库，避免个人信息的泄露、损坏或丢失。原则上信息化建设中的个人信息均需要在学校数据中心服务器本地存储，不得在校外、校内非数据中心环境中存储。

第十条 在学校信息化建设中，各信息化项目在使用个人信息时应严格遵循前款所述的合法原则、最小必要原则、安全原则和知情同意原则。

各信息化项目应严格按照数据资源使用申请中所确定的用途使用个人信息，严禁将个人信息挪作他用。因信息化建设工作需要，可接触到个人信息的相关人员，对相关个人信息负有保密责任，严禁未经授权对外提供个人信息。

各信息化项目中，对于个人信息的查询、修改等操作应保留不少于 180 天的最新操作日志，并提供审计功能，可审计对个人信息的各类操作。除个人信息的源数据系统，其他业务系统原则上禁止提供单独针对个人信息数据的批量导出功能。对个人信息的重要操作前（如批量修改、拷贝、导出等），需由相关数据主管部门信息化负责人与网信中心负责人共同审批，审批通过后方可进行操作。

各信息化项目应对必须要通过界面（如显示屏幕、纸面）展示的个人信息进行去标识化处理。个人信息去标识化的具体方法，请参考附件的校内个人信息去标识化参考指南处理。

在信息化建设中，依照本办法获取的个人信息，经过匿名化处理后无法识别特定个人且不能复原的，可直接应用于学校的科研、教学、校务管理等工作中，匿名化处理后的信息数据所有权及其相关知识产权归学校所有。

对于非学校信息化工作中的个人信息查询，原则上只接受公安部门等上级主管部门依法依规的查询请求，查询请求受理部门为相关个人信息数据主管部门，其他业务部门不得接受查询请求，

也不得进行个人信息查询和提供个人信息数据。

第十一条 校内其他非个人信息管理系统需使用个人信息时需充分评估合法性、必要性和安全性，只有缺乏相关个人信息就无法正常使用的系统，在安全性可以满足个人信息保护要求的前提下，可依法依规进行个人信息共享。非数据源的各业务系统原则上不得共享个人敏感信息。个人信息的数据共享交换工作按照《大连理工大学信息化数据资源管理办法》要求执行。

第十二条 在信息化建设中只有相关法律法规有明确规定需要公示的个人信息，才可进行公开。公开个人信息遵循最小化原则，通过信息组合能识别特定自然人身份并满足公示要求即可，严禁超范围公开其他相关信息，相关个人信息需进行去标识化处理，不得直接公开完整的个人信息。

对于以下个人敏感信息不宜公开，包括：银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息以及 14 岁以下（含）儿童的个人信息。

第十三条 注销的信息化项目或报废的存储设备，要确保承载的个人信息已被清理才可进行注销或报废处理。

对于违反法律法规及本办法采集、存储的个人信息，应依法依规删除相关个人信息数据。

第四章 责任认定及追责

第十四条 网信中心将依照本办法对各信息化项目中个人信

息处置相关的审计记录进行检查，或者通过其他网络安全检测手段检查个人信息的采集、存储、使用及处理情况。对于出现的违规行为将按照网络安全事件进行处置，校内相关部门及个人应按照本办法及相关整改通知，及时、彻底的整改相关问题。

第十五条 对于造成重大损失或整改不力的违规行为，由网信中心负责汇总相关情况，提交学校网络安全与信息化建设管理委员会及其下设的网络信息安全工作组进行责任认定，确定相关责任人、责任部门，按照学校网络安全管理办法等相关管理制度进行追责。对于违反国家法律法规的行为，学校将配合公安、网信等主管部门进行处理。

第五章 附则

第十六条 本办法由网络与信息化中心负责解释。

第十七条 本办法自发布之日起施行。

附件:

校内个人信息去标识化参考指南

在大连理工大学信息化建设中，如需对个人信息进行去标识化处理，应保证处理后的信息无法或很难进行复原，部分信息去标识化可参考以下方法进行:

姓名可隐藏名字中的 1-2 位;

出生日期可隐藏 2 位日期;

身份证件号码可隐藏结尾后 6 位;

学号、教工号可隐藏结尾后 3 位;

个人手机号可隐藏结尾后 4 位;

个人通信地址及家庭住址可隐藏具体门牌号;

车牌号可隐藏后五位中的任意 2-3 位。

上述未说明的个人信息应遵循不可复原原则进行去标识化处理。