LINCOLN COLLEGE

DATA PROTECTION POLICY

POLICY HR/PO/14

SPONSOR

Group Director of Human Resources

Last Updated: February 2019 Last Reviewed: February 2019 Next Review Period: 2019/20 academic year

Equality and Diversity Statement

Lincoln College strives to treat all its members and visitors fairly and aims to eliminate unjustifiable discrimination on the grounds of gender, race, nationality, ethnic or national origin, political beliefs or practices, disability, marital status, family circumstances, sexual orientation, spent criminal convictions, age or any other inappropriate grounds.

LINCOLN COLLEGE

DATA PROTECTION POLICY

CONTENTS

Para	Content	Page Number
1	Purpose	1
2	Aims	1
3	Introduction	1
4	Status of the Policy	2
5	Individual Rights	2
6	Data Security	4
7	Impact Assessments	4
8	Data Breaches	4
9	International Data Transfers	5
10	Individual Responsibilities	5
11	Training	5
12	Conclusion	6
Appendix 1	Guidelines for Retention of Personal Data	7
Appendix 2	Form for making a Subject Access Request	9
Appendix 3	Subject Access Request Procedure	10
Appendix 4	Form for reporting a Data Breach	11
Appendix 5	Data Breach Procedure Flowchart	13

LINCOLN COLLEGE

DATA PROTECTION POLICY

1 PURPOSE

1.1 Lincoln College is committed to being transparent about how it collects and uses the personal data of its workforce and students and to meeting its data protection obligations. This policy sets out the organisation's commitment to data protection together with individual rights and obligations in relation to personal data.

1.2 This policy applies to the personal data of job applicants, employees, workers, contractors, volunteers, interns, apprentices and former employees, referred to as HR-related personal data. This policy also applies to the personal data of students.

1.3 The organisation has appointed the Clerk to the Corporation as its Data Protection Officer. Their role is to inform and advise the organisation on its data protection obligations. The Clerk can be contacted at dpo@lincolncollege.ac.uk. Questions about this policy, or requests for further information, should be directed to the Data Protection Officer.

2 AIMS

The aims of the policy include the following:

- To explain the responsibilities of staff under the General Data Protection Regulation
- To explain the rights of individuals as data subjects
- To explain how data breaches are handled
- To provide information on the retention of data.

3 INTRODUCTION

3.1 Lincoln College needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, Lincoln College must comply with the following data protection principles which are set out in the General Data Protection Regulation (often known as GDPR):

- The organisation processes personal data lawfully, fairly and in a transparent manner
- The organisation collects personal data only for specified, explicit and legitimate purposes
- The organisation processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing

- The organisation keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay
- The organisation keeps personal data only for the period necessary for processing
- The organisation adopts appropriate measures to make sure that personal data is secure and protected against unauthorised or unlawful processing and accidental loss, destruction or damage.

3.2 Lincoln College and all staff, or others who process or use any personal information, must ensure that they follow these principles at all times. In order to ensure that this happens, Lincoln College has developed its Data Protection Policy.

3.3 Key definitions are detailed below:

- Personal data: is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it
- Special categories of personal data: is information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data
- Criminal records data: is information about an individual's criminal convictions and offences and information relating to criminal allegations and proceedings.

4 STATUS OF THE POLICY

4.1 This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by Lincoln College from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings, including dismissal.

4.2 Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the designated data controller initially. If the matter is not resolved it should be raised as a formal grievance.

5 INDIVIDUAL RIGHTS

As a data subject, individuals have a number of rights in relation to their personal data.

<u>Subject Access Requests</u>

5.1 Individuals have the right to make a subject access request. If an individual makes a subject access request, the organisation will tell him/her:

- Whether or not his/her data is processed and if so, why, the categories of personal data concerned and the source of the data if it is not collected from the individual
- To whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area and the safeguards that apply to such transfers
- For how long his/her personal data is stored
- His/her rights to rectification or erasure of data, or to restrict or object to processing
- His/her right to complain to the Information Commissioner if he/she thinks the organisation has failed to comply with his/her data protection rights, and
- Whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

5.2 The organisation will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

5.3 To make a subject access request, the individual should send the request to dpo@lincolncollege.ac.uk using the form at appendix 2. In some cases, the organisation may need to ask for proof of identification before the request can be processed. The organisation will inform the individual if it needs to verify his/her identity and the document it requires.

5.4 The procedure to be followed following a subject access request is illustrated on the flowchart at appendix 3.

5.5 The organisation will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the organisation processes large amounts of the individual's data, it may respond within three months of the date the request is received. The organisation will write to the individual within one month of receiving the original request to tell him/her if this is the case.

5.6 If a subject access request is manifestly unfounded or excessive, the organisation is not obliged to comply with it. Alternatively, the organisation can agree to respond but will charge a fee which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the organisation has already responded. If an individual submits a request that is unfounded or excessive, the organisation will notify him/her that this is the case and whether or not it will respond to it.

Other Rights

5.7 Individuals have a number of other rights in relation to their personal data. They can require the organisation to:

- Rectify inaccurate data

- Stop processing or erase data that is no longer necessary for the purposes of processing

- Stop processing or erase data if the individual's interest override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data)
- Stop processing or erase data if processing is unlawful, and
- Stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the organisation's legitimate grounds for processing data.

5.8 To ask the organisation to take any of these steps, the individual should send the request to dpo@lincolncollege.ac.uk.

6 DATA SECURITY

6.1 The organisation takes the security of personal data seriously. The organisation has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure and to ensure that data is not accessed, except by employees in the proper performance of their duties.

6.2 Where the organisation engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

7 IMPACT ASSESSMENTS

Some of the processing that the organisation carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the organisation will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

8 DATA BREACHES

8.1 If the organisation discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The organisation will record all data breaches regardless of their effect.

8.2 Any data breaches must be reported using the form at appendix 4. The DPO inbox is monitored on a daily basis. If the DPO is absent, the responsibility for checking the inbox will fall to one of the working group members.

8.3 If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

8.4 The procedure to be followed upon notification of a data breach is illustrated at appendix 5.

9 INTERNATIONAL DATA TRANSFERS

The organisation will not transfer student data to countries outside the EEA. The organisation will not transfer staff data to countries outside of the EEA, with the exception of staff that work in China where a CV is required to support the visa application process.

10 INDIVIDUAL RESPONSIBILITIES

10.1 Individuals are responsible for helping the organisation keep their personal data up to date. Individuals should let the organisation know if data provided to the organisation changes. For example, if a staff member moves house or changes his/her bank details, their iTrent Self-Service account should be updated.

10.2 Individuals may have access to the personal data of other individuals such as students. Where this is the case, the organisation relies on individuals to help meet its data protection obligations to staff and students.

10.3 Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction)
- not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device
- not to store personal data on local drives or on personal devices that are used for work purposes, and
- to report data breaches of which they become aware to the Data Protection Officer (Clerk to the Corporation) immediately.

10.4 Failure to observe these requirements may amount to a disciplinary offence, which will be dealt with under the organisation's disciplinary procedures. Significant or deliberate breaches of this policy, such as accessing employee or student data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

11 TRAINING

11.1 The organisation will provide training to all individuals about their data protection responsibilities as part of the induction process.

11.2 Individuals whose roles require regular access to personal data will have a mandatory requirement to complete data protection training.

12 CONCLUSION

Compliance with the General Data Protection Regulation is the responsibility of all members of Lincoln College. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, access to Lincoln College facilities being withdrawn, or even a criminal prosecution. Any question or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Officer.

APPENDIX 1

GUIDELINES FOR RETENTION OF PERSONAL DATA

Type of Data	Suggested Retention Period	Reason
Personnel files including training records and notes of disciplinary and grievance hearings.	6 years from the end of employment	References and potential litigation
Application forms/interview notes (for unsuccessful candidates)	At least 6 months from the date of the interviews.	Time limits on litigation
Redundancy details	6 years from the date of redundancy	As above
Income Tax and NI returns, including correspondence with HMRC	At least 3 years after the end of the financial year to which the records relate	Income Tax (Employment) Regulations 1993
Statutory Maternity Pay records and calculations	As above	Statutory Maternity Pay (General) Regulations 2014
Parental Leave	18 years from the birth of the child	Parental Leave Regulations 2013 Shared Parental Leave Regulations 2014
Statutory Sick Pay records and calculations	6 years from the end of employment	Statutory Sick Pay Regulations 2014
Wages and salary records	6 years	Taxes Management Act 1970
National Minimum Wage records	3 years after the end of the pay reference period following the one that the records cover	National Minimum Wage Act 1998
Accident books, and records and reports of accidents	3 years after the date of the last entry	RIDDOR 1995 Limitation Act 1980
Health records	During employment	Management of Health and Safety at Work Regulations
Health records where reason for termination of employment is connected with health, including stress related illness.	3 years	Limitation period for personal injury claims
Medical Records kept by reason of the Control of Substances Hazardous to Health Regulations	40 years from the date of the last entry	COSHH 1999 & 2002
Records of tests and examination of control systems and protective equipment under the Control of Substances Hazardous to Health Regulations (COSHH)	5 years from the date on which the tests were carried out	COSHH 1999 & 2002

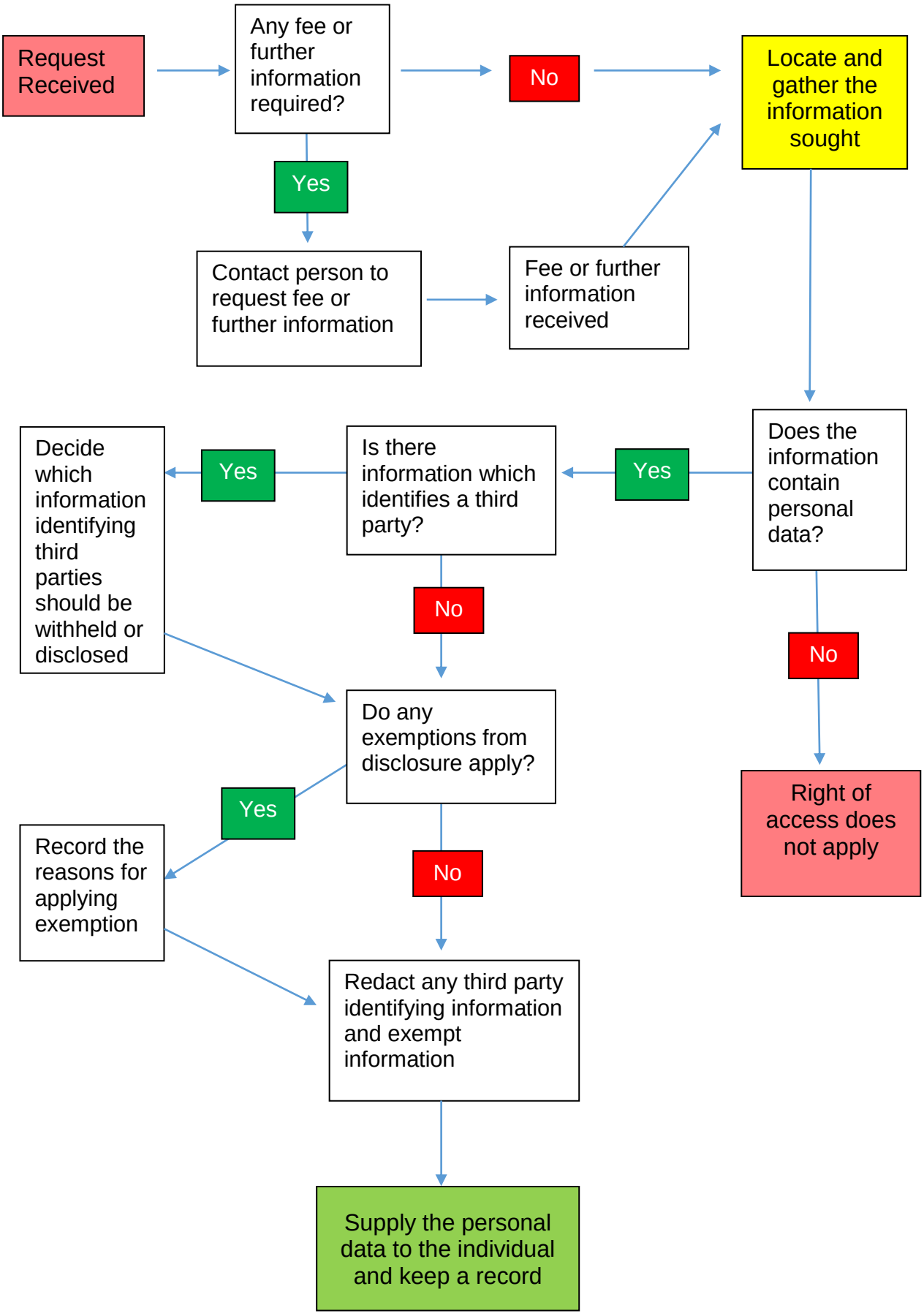
Medical records under the Control of Asbestos at Work Regulations Medical records containing details of employees exposed to asbestos Medical examination certificates	40 years from the date of the last entry 4 years from the date of issue	The Control of Asbestos at Work Regulations 2002 (SI 2002/ 2675). Also see the Control of Asbestos Regulations 2006 (SI 2006/2739) and the Control of Asbestos Regulations 2012 (SI 2012/632)
Medical records under the Ionising Radiations Regulations 1999	Until the person reaches 75 years of age, but in any event for at least 50 years	The Ionising Radiations Regulations 1999 (SI 1999/3232)
Student records, including academic achievements, and conduct	At least 6 years from the date the student leaves Lincoln College, in case of litigation for negligence. At least 10 years for personal and academic references, with the agreement of the student.	Limitation period for negligence
Records relating to Children & Young Adults	Until the child/young adult reaches the age of 21	Limitation Act 1980

APPENDIX 2

FORM FOR MAKING A SUBJECT ACCESS REQUEST

Name:
Daytime telephone number:
Email:
Address:
Employee/Student Number:
By completing this form, you are making a request under the Data Protection Regulation for information held about you by the college that you are eligible to receive
Required information (and any relevant dates): [Example: Emails between “A” and “B” from 1 May 2017 to 31 July 2017]
By signing below, you indicate that you are the individual named above. The organisation cannot accept requests regarding your personal data from anyone else, including family members. We may need to contact you for further identifying information before responding to your request. You warrant that you are the individual named and will fully indemnify us for all losses, costs and expenses if you are not. Please return this form to dpo@lincolncollege.ac.uk Please allow 28 days for a reply
Data subject’s signature:
Date:

APPENDIX 3 SUBJECT ACCESS REQUEST PROCEDURE



APPENDIX 4

FORM FOR REPORTING A DATA BREACH

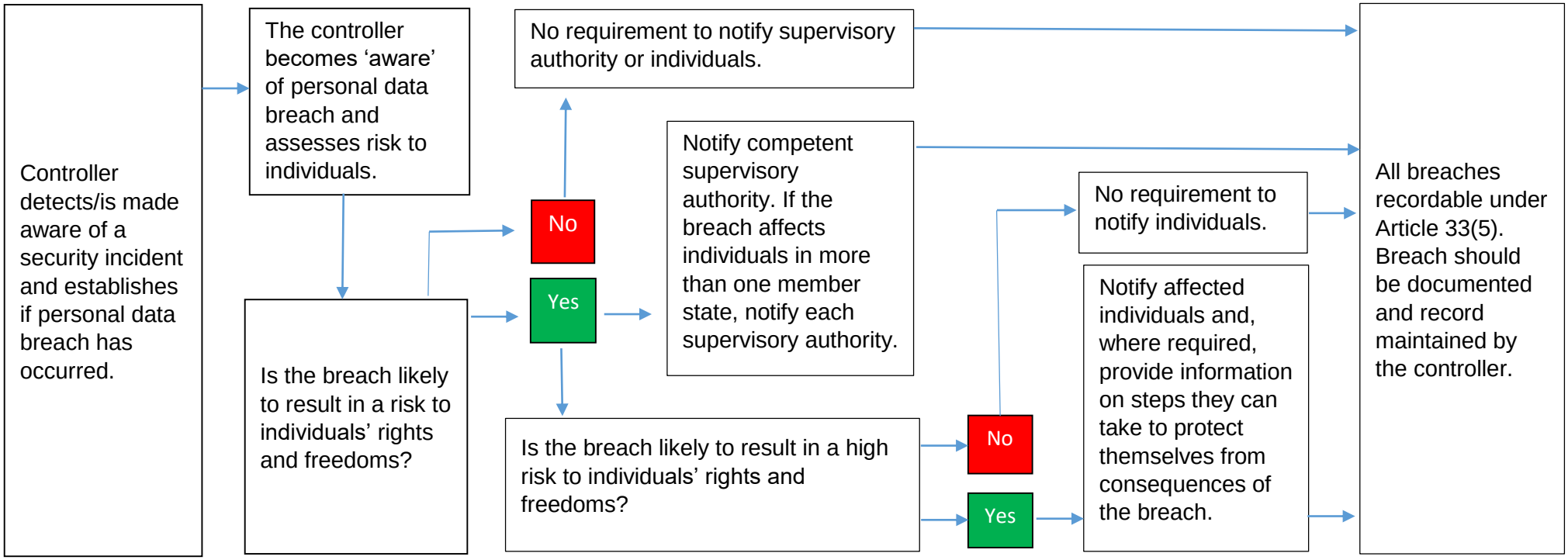
Please act promptly to report any data breaches. If you discover a data breach, please notify your Head of Department/School immediately, complete Section 1 of this form and email it to dpo@lincolncollege.ac.uk

Section 1: Notification of Data Security Breach	To be completed by the person reporting the incident
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name and Job Title of person reporting incident:	
Contact Details (email and extension number):	
Description of incident:	
Number of data subjects affected:	
Provide details of any personal data that has been placed at risk:	
Brief description of any action taken at the time of the discovery:	

Section 2: Action Taken	To be completed by the DPO
Incident Number:	e.g. year/001
Date of notification to Information Commissioner's Office (if relevant):	
Date of notification to data subject(s):	
Follow-up action required/recommended:	

APPENDIX 5

DATA BREACH PROCEDURE



A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

The ICO states: "A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors.

Once a breach is reported and an assessment carried out resulting in a risk to an individuals' rights and freedoms then the ICO must be notified. This must do this within 72 hours of becoming aware of the breach, where feasible, either by telephone or online outside of office hours