DOCUMENT DETAILS

Document Name:	Nottingham College Data Protection Policy
Document reference	See naming protocol
Version	1.3
Issue Date:	April 2019
Review Date:	March 2020
Document Author	Jo Welham
Document Owner	Jo Clifford
Applicability	All staff, volunteers and Governors of Nottingham College, all other parties under contract
Summary	The purpose of this document is to set out the policy for Data Protection at Nottingham College

DOCUMENT CONTROL

Version history			
Version	Date	Reason for release/version update	Issued by
1	24 January 2018	First draft	Michael Davies
1.1	5 February 2018	Update to principles and response time	Michael Davies
1.2	8 March 2018	Update following feedback from Board meeting 6 March 2018	Michael Davies
1.3	March 2019	Policy reached review date	Jo Welham, DPO

DOCUMENT APPROVAL

Approving person/body	Job Role (where applicable)	Date Approved
Board	Board	04/03/2019

COMMUNICATION

Date sent to OLT	04/04/2019
Date sent to Internal Comms	11/04/2019
Publication required on External Website?	No

CONTENTS

1. INTRODUCTION

1.1 Nottingham College is committed to preserving the privacy of the personal data of its staff and students through compliance with the Data Protection Act (2018) and the General Data Protection Regulation (EU) 2016/679 (GDPR) (collectively referred to as 'data protection legislation'). The College undertakes to process personal data responsibly, protect it and keep it secure. Nottingham College is on the Information Commissioner's Register of Data Controllers, reference no. Z700805X.

1.2 Personal data is data relating to a living individual who can be identified from it alone, or when it is combined with other information held by the College or which the College is likely to receive. This can include sensitive (special category) data relating to an individual's gender, age, ethnicity, disability, trade union membership, political opinions, religious or similar beliefs, physical or mental health, sexual life, or information relating to criminal proceedings or outcomes. The College has a procedure for processing special category and criminal conviction data specifically, in line with the DPA 2018.

1.3 Processing of personal information within the scope of the GDPR includes obtaining, storing, viewing, using, updating, disclosing and destroying any data held electronically, in structured manual records and to a limited extent in unstructured manual records.

1.4 Article 5 of the GDPR requires that personal data shall be:

- 1.4.1 Processed lawfully, fairly and in a transparent manner in relation to individuals
- 1.4.2 Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- 1.4.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- 1.4.4 Accurate and, where necessary, kept up to date
- 1.4.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- 1.4.6 Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

1.5 Nottingham College also complies with Freedom of Information legislation. This compliance is governed by the Freedom of Information policy.

2. OBJECTIVE

2.1 Nottingham College processes the personal data of its learners, employees, contractors, volunteers and associates to provide, produce or fulfil the following:

- 2.1.1 financial and staffing records including salary and benefits, holiday and sickness, performance and achievement

2.1.2 safeguarding and other statutory obligations relating to staff and students such as equality, diversity and inclusion and health and safety
2.1.3 education and support to learners and promotion of these services
2.1.4 funding claims and contractual obligations
2.1.5 publications
2.1.6 maintenance of the security of the premises and for the prevention or detection of crime (including CCTV)

2.2. This is not an exhaustive list. More information on processing of data subjects' information is provided in the College's Privacy Notices for students, staff and other groups.

3. RESPONSIBILITIES

3.1 All staff, volunteers and Governors of Nottingham College and all other parties under contract are expected to read this policy and to act in accordance with data protection legislation when handling the personal information of learners, staff and others associated with the College.

3.2. Any unauthorised disclosure of personal data to a third party by any staff member may result in disciplinary or legal action. Failure to comply with College policies and procedures for handling staff/student data is a disciplinary offence which may be considered gross misconduct and may also involve personal criminal liability.

4. POLICY STATEMENT

4.1. This policy outlines the responsibilities of all staff (including parties under contract, and or self-employed / volunteers) with regard to data protection legislation.

4.2. All staff, volunteers and Governors of Nottingham College and all other parties under contract are required to handle and process data in any of the College's records or systems in accordance with this policy and in accordance with other related policies concerning the handling or processing of data.

5. IMPLEMENTATION

5.1 To meet its responsibilities Nottingham College will:

5.1.1 Maintain up-to-date audits of where personal information is located within the College and how this is processed, including its sharing internally and externally
5.1.2 Ensure any new or planned projects that involve Personal Data are preceded with a Data Privacy Impact Assessment (DPIA)
5.1.3 Ensure any personal data is processed in a fair and lawful way and that only the minimum amount of information needed is collected and used
5.1.4 Ensure that any personal information processing has an identified legal basis and gain explicit consent where required

5.1.5 Explain at the outset why information is being collected, what it will be used for and with whom it will be shared

5.1.6 Ensure any information processed is up to date and accurate

5.1.7 Review the length of time information is held, in line with JISC recommendations and other relevant legislation, including disposing of data when appropriate

5.1.8 Ensure information is kept securely, including ensuring that system access controls are limited to role relevance

5.1.9 Ensure that data subjects can exercise easily their rights under data protection legislation

5.1.10 Ensure that anyone managing and handling personal information is trained to do so and is aware of how to report a data breach

5.1.11 Ensure that anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do

5.1.12 Ensure that any disclosure or sharing of personal information is in line with relevant legislation and internal policies and procedures

5.1.13 Take measures to ensure safe transfers of data outside of the EU/EEA where cross border sharing is necessary

6. DATA SECURITY

6.1 The College has an Information Security Policy that staff must adhere to in order to ensure personal information held on the College's network is protected from unauthorised viewing and from loss.

6.2 Where electronic files need to be shared, the following should be ensured:

6.2.1 Any sensitive personal information sent by email should be password protected as a minimum, with the password delivered to the recipient using a method other than email

6.2.2 Whenever possible, the information should be shared via a link from staff members' One Drives in Office 365

6.1 Paper records containing personal information should be minimised, but where these need to be kept the following should be carried out:

6.3.1 Use of lockable cupboards (with restricted access to keys)

6.3.2 Minimisation of personal data is taken off site and ensuring it is transported and stored as securely as possible

6.3.3 Correct use of confidential waste services

7. DATA SUBJECTS' RIGHTS

7.1 The College has two procedures governing its response to those who wish to exercise their rights with respect to their personal information:

7.1.1 the Subject Access Request Procedure

7.1.2 the Data Subject Rights Procedure – for all rights **other** than access

7.2 It is a criminal offence under the GDPR for any user to alter, illegally access, deface or remove any record (including e-mails) following receipt of an information request. The College will take necessary action against any individual who is found to have carried out this act, which may result in disciplinary or legal action. Other Criminal acts under GDPR may also result in disciplinary or criminal proceedings; definitions can be found at www.ico.org.uk

7.3 Any queries or concerns regarding Nottingham College's management of personal data should be managed through its complaints procedure. The College will maintain records of all complaints and their outcome. If they are still unhappy after having made a complaint individuals can contact the Information Commissioner through their website: www.ico.org.uk .

8. DATA SHARING

8.1 There are occasions when it is necessary for the College to share data with other organisations or people. Data Subjects will be informed of this, most usually through the College's Privacy Notices. Where consent is the legal basis for any data sharing, this will be collected in line with data protection legislation.

8.2 Where appropriate, a data sharing or processing agreement will be put in place, and due diligence carried out with respect to the recipient of the personal information.

9. RETENTION AND DISPOSAL OF DATA

9.1 The College will retain information about staff and students for as long as is reasonable and necessary to comply with the law and for legitimate business needs. This will include information needed in connection with administering pensions and taxation, for potential or current disputes or litigation regarding employment, in the case of job applicants, in relation to any complaints or claims regarding the selection process, and information required for job references.

9.2 For students this will include information needed in connection with administering student applications, enrolment, attendance, achievement, success, post-college destinations, personal tutor notes, academic records, and information required for references, and in the case of prospective students, in relation to any enquiries, applications and interviews.

9.3 The College will dispose of data in line with its Data Retention and Disposal Policy, which has been written in conjunction with JISC recommended data retention principles for Further Education, and legal and funding audit requirements. Once any retention period has elapsed, the College will ensure that information is destroyed by secure means, i.e. by shredding, pulping or burning for hard copy, deletion for electronic/digitised copy. The College uses a reputable ISO Accredited company for destruction where archived information has been sent off site, and destruction certification is received as appropriate.

10. DATA BREACH PROCEDURE

10.1. The College takes the risk of information loss very seriously. The College has a Data Breach Management Procedure to be followed in the event of a data breach or suspected data breach to ensure the College responds and manages effectively any breach in line with the GDPR.

11. REFERENCES

11.1 The following Policies and guidance are relevant to personal information:

- Social Media Guidelines
- Freedom of Information Policy
- Information Security Policy
- Data Breach Management Procedure
- Data retention and Disposal Policy
- Data Subject Access Request Procedure
- Data Subject Rights Procedure
- Procedure for processing special category and criminal conviction data
- Data Privacy Impact Assessment guidance
- Disciplinary Procedures for staff and students
- Equality, Diversity and Inclusion (EDI) Policy
- Safeguarding Policy

11.2 The College will adhere to its obligations under other legislation relevant to the use of personal data, which include:

- the Regulation of Investigatory Powers Act 2000;
- the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000;
- the Communications Act 2003;
- Data Protection Act 2018; and General Data Protection Regulation
- the Human Rights Act 1998;
- the Defamation Act 1996,
- the Equality Act 2010
- the Safeguarding Vulnerable Groups Act 2006.