DOCUMENT DETAILS

Document Name:	Nottingham College Data Protection & GDPR Policy
Document reference	GOV/COP/180306
Version	1.2
Issue Date:	24/04/2018
Review Date:	March 2019
Document Author	Michael Davies
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 and General Data Protection Regulation

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

DOCUMENT APPROVAL

Approving person/body	Job Role (where applicable)	Date Approved
Board	Board	6 March 2018

CONTENTS

1. INTRODUCTION 3
2. PURPOSE 3
3. DEFINITIONS 3
4. POLICY STATEMENT 4
5. IMPLEMENTATION 4
6. TRAINING 5
7. COLLEGE POLICIES AND LEGISLATIVE CONNECTIONS 5
8. DATA SECURITY 5
9. DATA SUBJECT RIGHTS / SUBJECT ACCESS REQUESTS 6
10. DATA SHARING 7
11. RETENTION AND DISPOSAL OF DATA 8
12. DATA SECURITY BREACH PROCEDURE 9

1. INTRODUCTION

Nottingham College is committed to preserving the privacy of its staff and students, and to comply with the Data Protection Act (1998) and the General Data Protection Regulation.

The data protection principles are set out in the Data Protection Act (1998). Article 5 of the General Data Protection Regulation requires that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date
- 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
- 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

2. PURPOSE

Nottingham College processes personal data to fulfil contractual obligations, salary and benefits, holiday and sickness, funding claims, performance and achievement, safeguarding, equality diversity and inclusion, health & safety, accident reports, disciplinary, provision of education, support and advice to the students and clients, to promote the services, for publications, financial and staffing records, and other statutory obligations. Processing of this data also includes the use of CCTV in order to monitor and maintain the security of the premises and for the prevention or detection of crime. This is not an exhaustive list.

3. DEFINITIONS

Personal data is defined as data relating to a living individual who can be identified from that data alone, or with other data held by the College or which the College is likely to receive. This includes sensitive 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, commission or alleged commission of any offence or information concerning related criminal proceedings or outcomes.

The GDPR regulates the "processing" of personal information which has a very broad meaning and includes obtaining, storing, viewing, using, updating, disclosing and destroying any data held electronically, in structured manual records and to a limited extent to unstructured manual records. The College is committed to using personal data responsibly to protect and keep secure from loss or destruction.

The requirements the College has for processing personal data are recorded on the public register maintained by the Information Commissioner. The College notify and renew the

notification on an annual basis as the law requires. If there are any interim changes, these will be notified to the Information Commissioner within 28 days. Nottingham College's registrayion with the Information Commissioner's Register of Data Controllers is : Z700805X, and can be found using this link : https://ico.org.uk/esdwebpages/search

4. POLICY STATEMENT

This policy outlines the responsibilities of all staff (including 3rd parties under contract, and or self-employed / volunteers) with regard to the Data Protection Act (1998) and the General Data Protection Regulation.

Staff 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

To meet the responsibilities Nottingham College will:

- Ensure any new or planned projects that involve Personal Data are preceded with a Data Privacy Impact Assessment.
- Ensure that access controls are limited to role relevance.
- Ensure any personal data is collected in a fair and lawful way.
- Gain explicit consent where required.
- Explain at the outset why information is being collected, what it will be used for and with whom it will be shared.
- Ensure that only the minimum amount of information needed is collected and used.
- Ensure the information used is up to date and accurate.
- Review the length of time information is held, in line with JISC recommendations and other relevant legislation.
- Ensure information is kept safely.
- Ensure the rights people have in relation to their personal data can be exercised.
- Dispose of data appropriate and without unnecessary delay.
- Ensure that anyone managing and handling personal information is trained to do so.
- Ensure that anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do.
- Any disclosure of personal data will be in line with relevant legislation, and internal policies and procedures.
- Any sharing of data to third parties is covered by a data sharing agreement.
- Take measures to ensure safe transfers of data outside of the EU/EEU where cross border sharing is necessary

6. TRAINING

Training relating to responsibilities and awareness of GDPR for Nottingham include the following:

- Induction mandatory training
- Annual on line testing
- In house risk assessment and audits

7. COLLEGE POLICIES AND LEGISLATIVE CONNECTIONS

The following Policies and guidance are relevant to personal information.

- Social Media Policy
- Freedom of Information Policy
- Information Security Policy
- Archiving Policy
- Data Privacy Impact Assessment guidance
- Disciplinary Policy
- Equality and Diversity Policy
- Safeguarding Policy

The College will adhere to its obligations under the Regulation relevant to the use and monitoring of electronic communications, which are predominantly:

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

8. DATA SECURITY

The College has an Information Security Policy that staff must adhere to in order to ensure personal information is protected from unauthorised viewing and from loss (including computer documents, emails and paper copies by ensuring staff are provided with adequate awareness training and follow guidelines set out in the GDPR code of practice:-

- Use lockable cupboards (restricted access to keys)
- Mandatory renewal of passwords to agreed frequency
- Password protection on personal information files
- Setting up computer systems to allow restricted access to certain areas

- Not allowing personal data to be taken off site (as hard copy, on laptop or on memory stick) without adequate safeguarding i.e. encryption
- If personal data can be taken off site, in which forms (paper, memory stick, and laptop) and give instruction to staff about keeping it safe
- Secure and reliable security back up of data
- Password protected attachments for sensitive personal information sent by email
- Robust and trustworthy IT security features
- Secure data flows across organisation and 3rd party data sharing requirements
- Robust secure on site IT storage facility of our electronic data
- Ensure all disposals of data are correctly destroyed using accredited organisations and appropriate certification is obtained.
- Ensure the use of confidential waste receptacles
- Ensure data is not shared without the explicit consent of the subject, where no exemptions apply.
- Set adequate access controls – role specific
- Take measures to ensure safe transfers of data outside of the EU/EEU where cross border sharing is necessary
- Continuous review of all measures

The College will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. All College users must take reasonable responsibility to ensure the data is accurate and up to date, relevant and not excessive. 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.

9. DATA SUBJECT RIGHTS / SUBJECT ACCESS REQUESTS

Individuals have a right under the Regulation to ask Nottingham College if it holds their personal data, and if so, be provided with a copy of it. Any person wishing to exercise this right should apply in writing to the College, or via the College website.

In order to ensure the College has met the Security requirements of the GDPR. The following information will be required before access is granted: (relevant identifying details including, Full name, Date of birth, National insurance number. The College may also require proof of identity. The following forms of ID will be acceptable: birth certificate, passport, or driving licence. Subject Access Requests will be dealt with in line with the GDPR recommended timescales. The College will aim to comply with requests for access to personal information as soon as possible, but will ensure it is provided within one month as required by the Regulation from receiving the written request. The College will provide the information in a clear format that is easily understood and in a format suitable for the requesters needs. The College may request further details to clarify the exact requirements prior to the start of the one month.

If an individual considers the details provided in response to a subject access request are incorrect or out of date, they should contact the College immediately.

Anyone whose personal information the College processes has the right to know:

- What information the College hold and processes about them
- The legitimate reasons for processing
- The right to consent or withdraw consent
- How to gain access to this information
- How to keep it up to date
- To receive this data in a clear format
- To receive this data within one month
- Data Subjects have the right to prevent processing of their personal data in some circumstances and have the right to correct, rectify, block or erase information regarded as incorrect
- To be informed of any miss use or loss of this data if the loss represents a high risk to the rights and freedoms of individuals
- The right to erasure of personal information – commonly referred to as the right to be forgotten
- The right to complain and/or seek compensation

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

If you have any queries or concerns regarding Nottingham College's management of personal data then you can contact the College directly.

Any comments or complaints will be dealt with through the College complaints procedure. The College will maintain records of all complaints and their outcome.

If you are still unhappy after having made a complaint individuals can contact the Information Commissioner through their website: www.ico.org.uk .

10. DATA SHARING

There are occasions when it is necessary for the College to share data with other organisations or people and where consent is required the College will seek and gain this from the Data Subject except where exemptions apply i.e.:

- In order to fulfil legal obligations
- In the vital interests of the individual

- Pay and benefit details HM Revenue and Customs
- UK Border Control
- Police or other Law enforcement or investigatory institutions
- Professional bodies e.g. solicitors. GPs Child protection agencies
- Other Educational bodies or institutions
- Futures / Connexions
- Education and Skills Funding Agency
- Internal and external audit
- Research purposes where data has been fully anonymised.

For further information, access the website of the Information Commissioner's Office: https://ico.org.uk/

Nottingham College is also required to comply with Freedom of Information legislation. This requires the college to implement a publication scheme setting out what information Nottingham College routinely publishes, and to publish information according to that scheme (or in relation to any environmental information that it holds). A copy of the College's Publication Scheme is available on the Nottingham College website.

The College is also required to deal with individual requests under the Freedom of Information Act. It is the College's policy to be as transparent as possible with the information that it holds, whilst taking due account of the interests of data subjects where information requested contains personal information. As such, each request is considered on an individual basis.

11. RETENTION AND DISPOSAL OF DATA

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.

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.

The College will dispose of data in line with the College Data Retention Policy written in conjunction with JISC recommended data retention principles for Further Education, any legal and funding audit requirements. Once the retention period has elapsed, the College will ensure that any information is destroyed by secure means, i.e. by shredding, pulping or burning for hard copy, deletion etc. for electronic/digitised copy. The College will use a reputable ISO Accredited company and obtain destruction certification.

12. DATA SECURITY BREACH PROCEDURE

The College takes the risk to security loss very seriously and adheres to the legal framework set down by the Information Commissioner's Office and industry standards. The College has a 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 recommendations. Actions may include:

- Containment and recovery – the College will respond to the incident immediately which includes a recovery plan and, where necessary, implement procedures for damage limitation.
- Assessing the risks – the College will assess any risks associated with a breach, as these could affect any procedures after the breach has been contained. In particular, the College will assess the potential adverse consequences for individuals; how serious or substantial these are; and how likely they are to re occur.
- Notification of breaches – if appropriate the College will inform a Data Subject about an information security breach, the ICO; other regulatory bodies; other third parties such as the police and the banks; or the media.
- Evaluation and response – the College will investigate the cause of the breach and also evaluate the effectiveness of any response made. If necessary, the College will update its policies and procedures accordingly.