WELLINGTON COLLEGE
SPONSOR OF
WELLINGTON COLLEGE ACADEMY TRUST

DATA PROTECTION POLICY

This policy is applicable to all students, staff and parents of The Wellington College Academy Trust.

DOCUMENT CONTROL	
Responsible position:	**Approved by:**
Finance and Operations Director / IT Director	Executive Headteacher
Version number:	**Date approved:**
5.0	May 2018
Review Period:	**Next review date:**
3 years	May 2021

RELATED POLICIES AND DOCUMENTS	
Policy Name	**Date Issued**
Data Protection Act	July 1998
E-Safety Policy	May 2013
Freedom of Information Act	November 2000
Safeguarding and Child Protection Policy	February 2013
Safer Recruitment and Selection Policy	June 2013
Transfer of Undertakings (Protection of Employment) Regulations	February 2006
General Data Protection Regulation (GDPR)	May 2018

REVISION RECORD		
Date	**Version**	**Revision Description**
September 2009	1.0	Written in line with current legislation and policies
June 2013	2.0	Amended in line with updated Safeguarding and Child Protection Policy and legislation acts
June 2014	3.0	Amended in line with updated Safeguarding and Child Protection Policy and transfer to MAT
January 2017	4.0	Reviewed and Updated in line with current legislation
May 2018	5.0	GDPR Additions

1. INTRODUCTION

1.1 The Wellington College Academy Trust ("the Trust") will hold and process confidential, personal and sensitive personal information about people, such as names and addresses of staff and students, families, health and other private matters.

1.2 This policy is designed to assist in the avoidance of a breach of both the Data Protection Act 1998 ("DPA") and the General Data Protection Regulation(GDPR) which comes into force on 25th May 2018. The DPA provides strict rules in this area and the GDPR even stricter rules and penalties.

1.3 This policy is designed to be used by, senior staff, HR, line managers, teaching and support staff and administrative staff, and students within The Trust and its Board of Directors and members of the local governing body.

1.4 Please also refer to the Wellington College Academy Trust IT Acceptable Use Policy.

2. DATA PROTECTION OFFICER

2.1 The Trust's Data Protection Officer is contactable via dpo@wcat.org.uk.

2.2 If you are in any doubt about what you may or may not do, seek advice from the Trust's Data Protection Officer.

3. DEFINITIONS

3.1 "Personal Data": Personal data is information relating to a living individual who can be identified from those data or from those data and other information which is or might become available to anyone in the Trust, or anyone we do business with.

3.2 "Special Category (Sensitive) Personal Data": Some personal data is classed as special category personal data. This type of data is subject to further regulations under the GDPR and can only be processed under certain circumstances.

Personal data becomes sensitive if it includes any of the following types of information about an identifiable, living individual:

- racial or ethnic origin;
- political opinions;
- religious beliefs;
- trade union membership;
- physical or mental health;
- sexual life;
- commission of offences or alleged offences.
- Biometrics (used for ID purposes)

4. THE GENERAL DATA PROTECTION REGULATION

4.1 The DPA and GDPR requires that all personal data must:

- be fairly and lawfully processed;
- be processed for limited purposes and not in any manner incompatible with those purposes;
- be adequate, relevant and not excessive;
- be accurate;
- not be kept for longer than is necessary;
- be processed in accordance with individuals' rights;
- be secure; and
- not be transferred to countries without adequate protection.

The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with these principles".

5. EXAMPLES OF DATA

Sensitive personal data is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically add the processing of genetic data, biometric data and data concerning health matters.

5.1 The following are examples of personal data and sensitive personal data kept by the Trust on members of staff:

- Full name
- Home address
- Home or contact telephone number
- National Insurance Number
- Bank account details (where appropriate)

5.2 During an employee's service other personal information about them is accumulated including:

- Employment application form, Curriculum Vitae and references
- Sickness records
- Annual, special, unpaid and compassionate leave records
- Personal appraisal and assessment records
- Training records
- Disciplinary records
- Promotion and transfer records
- Accident and injury at work records

Data includes both paper and electronic records.

These lists are not exhaustive and items can be added or deleted at any time.

6. HANDLING AND RETENTION OF RECORDS

6.1 When handling and retaining personal information the Trust undertakes to:

- Respect the privacy and human dignity of all subjects
- Limit intrusions of any kind to reasonable actions in circumstances where they can be justified
- As far a possible obtain personal data from the employee concerned on the basis of "informed consent"
- Minimise the amount of personal data held throughout the Trust
- Collect personal data only for justified reasons, e.g. emergency contact
- Control access of personal data so it is strictly "need to know" basis
- Ensure that all personal data processed by third parties e.g. Payroll / Occupational Health Provider is carried out to the Trust's own standards
- Inform employees joining the Trust that you hold personal data about them on file and the purpose of holding that data. Also advise them of their rights under the DPA
- Consent may be required for the processing of personal data unless processing is necessary for the performance of the contract of employment. Any information which falls under the definition of personal data and is not otherwise exempt, will remain confidential and will only be disclosed to third parties with appropriate consent.

7. DATA SECURITY

The Trust will take appropriate technical and organisational steps to ensure the security of personal data. All staff will be made aware of this policy and their duties under the Act.

The Trust and therefore all staff and pupils are required to respect the personal data and privacy of others and must ensure that appropriate protection and security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to all personal data.

An appropriate level of data security must be deployed for the type of data and the data processing being performed. Personal data must be stored in appropriate systems and be encrypted when transported offsite. Other personal data may be for publication or limited publication within the College, therefore having a lower requirement for data security.

Attention is also drawn to the existence of the *ICT Policy*, which provides more specific information on digital data protection within the ICT policy, and best practice guides that are published and updated on 365.

8. ACCESS TO PERSONAL INFORMATION

7.1 An individual employee has certain rights under the GDPR with regard to the information held about them. These are:

- The right to access to the information held about them
- The right to know that the company is processing the information, what information is being processed, why it is being processed and to whom it may be disclosed
- The right to prevent direct marketing using the information held about them

- The right to have personal information corrected
- The right to compensation if they are affected by errors in the information held
- The right to prevent automated decisions being made by a computer based upon the information held

7.2 An individual has the right to view the data held by the Trust about them and to amend it at any time when their personal circumstances change.

9. DISCLOSURE OF PERSONAL INFORMATION

8.1 The personal information held by the Trust about employees will only be disclosed to those within the company who are authorised to have access to it and only then if that disclosure is directly connected to their normal duties.

8.2 The following staff are authorised to have access to employee personal information:

- Executive Principal/Headteacher and Executive Principals Personal Assistant – all information
- Member(s) of Human Resources dealing with personal matters – all information
- Line managers – leave, appraisal and training information only
- The Trust's Occupational Health advisers

8.3 Personal information held by the Trust may also be disclosed to outside agencies such as the Police and HM Revenue and Customs, but such disclosure is only made under certain circumstances defined in the DPA.

8.4 In the event that the Transfer of Undertakings (Protection of Employment) Regulations 2006 apply so far as is possible data will be supplied in an anonymous form and if that is not possible, then the prospective employer will be required to keep such information confidential. The employee to whom the information refers is to be informed of the nature and means of such a disclosure.

8.5 The internal transmittal of personal information between authorised members of staff must be made in such a way that the information cannot be seen by those who are not authorised to see it. As a general rule this should be by means of a properly marked sealed envelope. Where this is not possible or impractical and personal information is to be transmitted by fax or e-mail, the following precautions must be taken:

- The transmittal of personal information should only be made over a secure network or by comparable means, or if e-mail is used, then by encryption.
- Where transmittal is made by fax, the transmittal is to be made by prior arrangement and the assigned recipient is to personally monitor the arrival of the fax at its destination.
- All copies of faxes or e-mails held by both senders and recipients are to be retained securely.
- Senders and recipients are responsible for ensuring that e-mails containing personal information about employees are deleted from the e-mail accounts at the earliest opportunity.

10. RETENTION OF RECORDS

9.1 It is necessary for a number of statutory reasons or for reasons of continuity, that the Trust must retain a certain amount of personal information about current and former employees. The following information is recommended by the Information Commissioner in its Employment Practices Data Protection Code for periods which information is to be retained. This available by emailing the data protection office on dpo@wcat.org.uk.

Any data protection queries should be addressed to the Data Protection Officer.

11. MONITORING OF EMAIL AND INTERNET COMMUNICATION

10.1 The Trust monitors e-mails and internet communications and activity. Further information can be found in the IT Acceptable Use Policy.

12. DISCIPLINARY ACTION

11.1 The access to personal information about an employee by any member of staff who is not authorised to do so will be treated as a matter of gross misconduct and will be subject to disciplinary action. Such access is also a criminal offence under the DPA.

11.2 The unauthorised disclosure of personal information about an employee to any person not authorised to receive it will be treated as a matter of gross misconduct on the part of the person disclosing the information and the person receiving it, and will be subject to disciplinary action pursuant to the Trust's Disciplinary Policy.

12 CCTV

The Trust owns and operates a CCTV network for the purposes of crime prevention and detection, and Safeguarding.

Where a data subject can be identified, images must be processed as personal data.