CONFIDENTIALITY OF STAFF INFORMATION POLICY

[applies to all Trust employees]

1. Introduction

The purpose of the policy is to ensure that all employees are aware of and understand the standards that BCUAT expects and requires in relation to confidentiality of staff information. This policy should be read in conjunction with the Data Protection Policy.

2. Scope

This policy applies to all employees of Birmingham City University Academies Trust (BCUAT), including employees working in academies operating as part of the Trust and all Head office employees.

3. Principles

Any personal information given or received in confidence for one purpose must be kept confidential under the Data Protection Act 1998. Disclosure of personal information must be controlled according to legal and professional obligations.

The term "person identifiable information" refers to information held regarding staff which identifies them personally. This includes, but is not limited to:

- Name, address, full postcode, date of birth, NI number, payroll number
- Pictures, photographs, videos, audio recordings, any other images

"Sensitive personal data" refers to additional information that the employee may have provided voluntarily such as ethnic origin, religious beliefs, disability, political opinions, actual or alleged offences, membership of a trade union.

All person identifiable information and sensitive personal data collected or processed by the Trust, and held in any medium, is confidential.

This policy applies to all Trust employees, and particularly to those who come into contact with confidential staff information during the course of their duties, including but not limited to:

- Human Resources staff
- Payroll staff
- Finance staff
- Line managers
- Academy Business Managers and administrative staff

Owner of Policy	Human Resources
Legislation Status (Statutory / Non-Statutory)	Non-Statutory
Date Ratified and Version Number	29.11.2016 v2.0
Date to be reviewed	September 2017

4. Confidentiality Commitment

The Trust guarantees to preserve the confidentiality of personal staff information it holds by making the following commitments:

- Confidential information will be held securely whether in hard copy or digital form
- Information held in personal files will be available for inspection by the member of staff to whom it relates
- Statutory authorities will be the only bodies (providing they have the appropriate judicial authority) able to examine files
- Information will be released to third parties only with the written agreement of the member of staff to whom it relates, with the exception of mandatory pre-employment checks such as DBS where consent is implied
- Human Resources staff, and other staff handling confidential staff information in the course of their duties, will at all times adhere to the principles of the data protection legislation relevant to staff records
- Policies and procedures relating to the handling of confidential information will be reviewed on a regular basis to ensure continued compliance with legislation and where possible to demonstrate best practice
- Trust staff will be made aware of the consequences of breaching confidentiality

5. Responsibilities

All staff should ensure they have read this policy and the Data Protection Policy and are aware of the procedures to be followed and the consequences of failing to do so. Every individual has a responsibility to safeguard the security and confidentiality of any personal information they hold. Any questions or concerns relating to these policies should be addressed to the HR Consultant.

Staff working with confidential staff information are responsible for ensuring that it is kept safe and secure at all times and that complete confidentiality is safeguarded. They are also responsible for compliance with all Data Protection requirements, including ensuring that only relevant and appropriate information is recorded and that access is restricted to those who have a valid reason for requiring access.

The HR Consultant is responsible for ensuring continued compliance with legislation and best practice and will review this policy and the Data Protection Policy at least annually. They will also update related procedures and documents such as the Code of Conduct and contracts of employment, ensuring that the importance of adhering to procedures relating to staff confidentiality and the consequences for failure to do so are clearly stated. They are responsible for ensuring that policies are made available to all staff, dealing with queries and providing any necessary training. In particular, they must ensure that staff responsible for managing and processing confidential staff information are aware of the procedures for doing so in adherence to the Data Protection Act.

The Trust Board is ultimately responsible for ensuring that the Trust complies with the Data Protection Act and will have in place a suitably robust schedule for policy review to ensure that this policy and the Data Protection Policy are reviewed at least annually

6. Use of personal information

Trust staff with relevant responsibilities may refer to your personal record throughout your employment with the Trust. Uses could include:

Activity	Staff with responsibility
Payment of monthly salary and pay reviews	HR, Payroll
Absence monitoring	HR, Academy administrative staff
Performance management	Line Manager, HR
Provision of pension estimates	Payroll
Provision of references	HR, Line Manager
Equal Opportunities monitoring	HR
Recruitment	HR, Line Manager, other managers

All information accessed or processed as part of these activities will remain confidential.

7. Passing on confidential information

Confidential information may only be passed on to someone else **with the subject's consent.**

Information may only be passed on to a third party for a justifiable purpose and only the minimum information required should be included.

Wherever possible subject information should be anonymised (i.e. the person's identity and other identifying details removed) or aggregated (statistics compiled from personal information – for example, equal opportunities monitoring).

An example of where the Trust may need to pass on confidential information is a referral to Occupational Health – this would only be done with the individual's consent.

8. Maintaining confidentiality

The confidentiality of staff information can be protected in a number of ways:

Procedures:

- Induction for all staff to include introduction to appropriate policies and the Code of Conduct
- Information to be recorded accurately and consistently
- Paper files to be kept in secure location with access limited to those with responsibility for processing the information
- Electronic files to be kept on network drives with access limited to those with responsibility for processing the information, or using password protection
- Ensuring that documents relating to staff are kept private, for example documents not left on public printer or left open on screen where others can see the information
- Disclosing and using information appropriately and with care – if in doubt, check with the HR Consultant first

Staff communication:

- Regular effective communication to all staff to ensure they are aware of requirements for the safekeeping and disclosure of information
- Keep information confidential by taking care when discussing staff issues in public places or in the presence of other members of staff
- Never discuss confidential information on social networking sites such as Twitter and Facebook

9. Breach of confidentiality

Every Trust employee has a responsibility to safeguard the security and confidentiality of personal staff information they hold, as stated in the Code of Conduct.

Any breach in the confidentiality of personal information would constitute a failure to comply with this policy and the Code of Conduct and could lead to action under the Disciplinary Procedure. There is also a risk of legal action by others.

10. Management of records

Personal files will be reviewed on a regular basis to ensure that only necessary and relevant information is retained, in line with statutory and recommended retention periods.

Any outdated hard copies to be destroyed will be shredded by those employees responsible for keeping the information secure and confidential, or using a secure external shredding service which complies with the Data Protection Act and our procedures relating to confidential information.