Directorate for Resources
HR and OD

Service Director: Sarah Keyes
Buckinghamshire Council
The Gateway
Gatehouse Road
Aylesbury
HP19 8FF
www.buckinghamshire.gov.uk

BC Confidentiality Statement

1 This statement applies to all workers (staff members / volunteers) in the Council as appropriate to their duties.

2 In the course of his or her duties a worker is likely to have access to a considerable amount of personal information relating to clients, staff, contacts or Members. Buckinghamshire Council (BC) emphasises that its workers must preserve confidentiality of information. All information is confidential within the Council and should only be provided on a 'need to know' basis. It is expected that all members of Children's Services and Adults and Family Wellbeing Services understand the importance of treating information in a discreet and confidential manner in accordance with professional codes of conduct..

3 The Council expects all workers to read and comply with the Council Information and Communication Technology Security Policy. Full details are available on the Council's Intranet.

4 The Council is under a legal duty to process personal information in accordance with the Data Protection Act 1998 and to respect the confidentiality of details held. All workers have a duty to manage knowledge and information in accordance with this legislation. Further details on the Data Protection Act and the Caldicott Principles may be found on the Council's Intranet.

5 Any misuse of information including a breach of this confidentiality agreement, or the underlying policies it refers to, is a serious matter and may result in disciplinary proceedings including dismissal without notice. Criminal matters may also be referred to the police. Further details on the Council Conduct and Discipline Policy can be found on the Intranet.

6 Access to electronic records may be monitored by the Council. This includes accessing, updating and amending files.

7 Any information on Council systems may only be disclosed to an authorised person. No data should be released until the rights of an enquirer to seek such information have been confirmed and recorded. If in doubt contact your line manager.

8 Under no circumstances must workers access any records unless they have a responsibility to do so as part of their duties/contract of employment. If this involves accessing personal information about a family member, friend or acquaintance, then you are under a duty to report this fact to your line manager and seek their written

consent to you accessing this data.

9 If workers become aware that they know a service user/client and/or family it is their responsibility to inform their line manager immediately so that appropriate arrangements can be made regarding the access to these particular records.

10 When recording information it must be clear whether it is factual or a professional opinion. Records should be free of jargon. The file may be the main historic source of information about significant events, decisions and people in individual service users' lives. Individuals are entitled to request to see information recorded about them and records should always be written with this in mind. Where appropriate, e.g. assessments, plans and reports, all parties' views should be recorded. Be aware that records marked as 'confidential' will be assessed when requested by clients to decide whether they continue to remain confidential.

11 All conversations relating to confidential matters (service users, employees, contracts, etc) should take place in a confidential setting and not where they could be overheard e.g. in corridors, lifts, cafes, etc.

12 E-mail correspondence must meet the same confidentiality principles as for all other written correspondence and be marked as confidential where appropriate. Great care must be taken in sending documents via external e-mail as it is not a secure means of communicating confidential information.

13 In line with the Council's policy, all confidential or personal paper documentation and portable media equipment (e.g. blackberries, memory sticks and laptops) should be stored securely when not in use. Portable media equipment should be password protected. Memory sticks should not be used unless encrypted.

14 In the event of data being lost or stolen, please inform your Line Manager who will take appropriate action in line with the Council's Data Breach Policy.

15 All documentation with service user, employee personal information or contract data should be disposed of as confidential waste.

16 IT log on details will not be issued to workers until they have discussed, understood, agreed to comply with and signed this confidentiality statement.

17 Passwords must not be shared. Workers are responsible for all transactions recorded under their logon. Likewise workers need to be aware of and prevent anyone who is not authorised to do so, having visual access to their computer screen. Further details on the Council's Password Policy can be found on the Intranet A-Z.

18 When working remotely (and in accordance with the Home Working Policy), the above principles still apply. Make sure you delete all copies of data held locally on your PC when you finish.

19 If you have concerns that another worker, or workers, may be in breach of the confidentiality standards set out in this statement, then these must be referred to your line manager. There is also a Council Whistle Blowing procedure for reporting concerns.

20 As a general point, confidentiality cannot always be guaranteed in relation to our overriding duty to protect children, young people and vulnerable adults from significant harm. If, in the course of their duties, a worker has concerns that a child, young person

or vulnerable adult may come to significant harm, then this concern must be reported. Social workers must report concerns about significant harm to their line manager. All other workers should report concerns about significant harm to children or young people, to the Local Authority Designated Officer for Child Protection. Concerns about significant harm to vulnerable adults should be reported to the Head of Safeguarding (CHASC).

21 If you have any questions or are uncertain about the meaning of any part of this notice you are expected to speak to your line manager and ask for any necessary explanations.

I have understood the above points and I agree to comply with these requirements.

I understand that any misuse of information including a breach of confidentiality, is a serious matter and may result in disciplinary proceedings including dismissal without notice under the Council's Conduct and Discipline Policy.

Name	
Job Title	
Signature	
Date	