

THE MILTON KEYNES CHILDREN'S CONTACT CENTRE

POLICIES AND PROCEDURES

Correspondence address:

MKCCC
PO Box 1549
BEDFORD
MK43 6AX

Contact Centre Address:

The Rowans
13A Moorfoot
Fullers Slade
Milton Keynes
MK11 2BD

Table of Contents

A. Notes of Guidance for Volunteers/Staff	3
B. Volunteer Policy	5
C. Volunteer Profile	7
D. Basic Tasks for a Volunteer	8
E. New Child Contact Centres and New Workers.....	9
F. Training Volunteers and Staff.....	10
G. Supporting Volunteers.....	11
H. Policy Statement on the Recruitment of Ex-offenders ...	12
I. Grievance Procedure for volunteers	14
J. Diversity Policy	15
K. Equal Opportunities Policy	16
L. Confidentiality Policy.....	17

M Complaints Policy and Procedure 18

N Domestic Violence and Conflict Management Policy 20

O Essential Requirements for Volunteers and Staff in Relation to Managing Domestic Violence and Conflict .. 21

P Photograph Policy 22

Q Exclusion Policy 23

R. Exclusion Policy Procedure 24

S Health and Safety Policy..... 25

T Child Protection / Safeguarding Children Policy 28

U Policy Statement: Data Protection Policy 32

V. Policy for Disclosure & Barring Service (“DBS Policy”) .. 33

W Privacy Policy 35

X Security Incident Response Procedure..... 38

Y Private Impact Assessment..... 43

Z Information Security Policy 45

AA Personal Commitment Statement for Volunteers..... 57

A. Notes of Guidance for Volunteers/Staff

1. It is hoped that it will not be necessary to ask volunteers/staff to be on duty more often than once in four weeks.
2. In order to "prepare" the Centre, volunteers/staff are asked to arrive at 10.00am. Please allow for an extra half an hour after the Centre has closed for a de-briefing session and for clearing up.
3. Three or more volunteers/staff will be on duty during each session and they will be expected to remain on the premises during the period when the Child Contact Centre is open to the public.
4. To ensure the smooth running of the Child Contact Centre volunteers/staff are asked to inform the Co-ordinator if they are unable to attend an allocated session, giving as much notice as possible.
5. The volunteer at reception must note the arrival and departure times of all clients.
6. Volunteers/staff should remember that parents are responsible for the safety and supervision of their children at all times - so that means that the non-resident parent cannot go out for cigarette or to make a mobile phone call. They must remain on the premises at all times with their child.
7. All volunteers/staff must wear a name badge (first name only) so that families can see immediately who is a worker at the Child Contact Centre.
8. Particular attention should be paid to new families attending the Child Contact Centre for the first time. Please go through the pre visit form and the parents' information leaflet with new families. You must ensure that no confidential information such as an address or telephone number is revealed to the other parent.
9. If it is apparent that there is, or is likely to be, conflict between family members during the contact session, an early opportunity should be taken to defuse the situation. If the matter cannot be resolved in the public area, one or both of the parties concerned should be asked to go to a private area. If the problem still cannot be resolved both parties should be advised to raise the matter with their respective referring agency. A volunteer should always be present when a private area is used by families.
10. In the event of a situation arising upon which the volunteers/staff on duty agree that they need further advice or help, there are a number of steps which can be taken:
 - 10.1 Attempt to contact the Centre Co-ordinator if he/she is not already present.
 - 10.2 If you feel that there is still no immediate solution ask the clients to leave the premises and advise them to contact their referring agency as a matter of urgency.
 - 10.3 If they refuse and their continuing presence represents any danger to them or to other users of the Child Contact Centre, contact the Police. Dial 999.
11. Volunteers/staff will be aware that what happens during a contact session is confidential. Confidentiality must be observed by all volunteers at all times. Any urgent concerns which volunteers may have should be shared with the Co-ordinator or Team Leader as soon as possible after the session.
12. Clients should be made aware that smoking is not permitted during the contact session and that any client arriving at the Child Contact Centre under the influence of alcohol or drugs will not be admitted and the contact for that session will be cancelled. These precautions are in the interests of all clients and particularly those of the children.
13. We believe it to be advisable that the parent attending for contact should spend the contact time with the child on their own. If the other parent wishes to stay at the Child Contact Centre in the early days of contact, they should be encouraged to refrain from being involved with contact during the session. If the parent chooses to leave the Child Contact Centre during contact, they should be encouraged to return not earlier than 5 minutes before the end of the

session, unless by mutual agreement. Each case will need to be treated on its merits, depending upon the level of emotional stress caused by the commencement of contact.

14. Volunteers/staff should not pass letters, messages, or parcels between parents. If money is involved, then accusations could be made that the other party did not receive it and the volunteers could be blamed. If a letter is passed across, the Volunteer would not know what was in it - it could be a threat. Volunteers are not 'go-betweens' - they put into practice agreements made elsewhere. They are there to facilitate contact - not to get involved.
15. **Volunteers/staff must not:**
 - 15.1 pass messages, parcels or letters between parents;
 - 15.2 physically restrain anyone;
 - 15.3 'look after' a child while the parent goes out for a cigarette or to make a phone call;
 - 15.4 take a child to the toilet, unless the parent asks for assistance and there is another volunteer present;
 - 15.5 Discuss the families outside of the Child Contact Centre.

B. Volunteer Policy

1. Milton Keynes Children's Contact Centre offers a facility where children of separated families can enjoy contact in a neutral meeting place with one or both parents, and sometimes other family members, in a safe and comfortable environment. In order to offer this service, volunteers are needed to:

- 1.1 Coordinate the service (if the Coordinator is voluntary);
- 1.2 Keep attendance records;
- 1.3 Serve refreshments;
- 1.4 Prepare and clear up the Centre on the day;
- 1.5 Ensure that the Centre is secure and safe;
- 1.6 Be on hand to assist the families using the Centre.

2. Recruitment

- 2.1 We will use appropriate means to advertise for volunteers locally that take into account the principles of our Equal Opportunities and Diversity Policies. The applicant will have to complete an application form, but help can be given with this if necessary. The applicant will be interviewed by the Coordinator and if this is successful the two references asked for will be taken up.
- 2.2 An enhanced level criminal records Disclosure with the Criminal Records Bureau will be made for every volunteer working in a Child Contact Centre.

3. Induction and training

- 3.1 There will be an induction prepared and delivered by the Coordinator or Team leader. This will include:
 - 3.1.1 The role of the volunteer.
 - 3.1.2 A list of all staff members and volunteers.
 - 3.1.3 A list of Management Committee members and sub-committees.
 - 3.1.4 Copies of all the Child Contact Centre policies including this volunteer policy and those on Child Protection, Confidentiality, Health and Safety, Equal Opportunities and Diversity, Domestic Violence and Conflict Management.
 - 3.1.5 Essential procedures i.e. timekeeping, rota etc.
 - 3.1.6 Details of on-going training including the requirement to undertake NACCC training modules over a three year period
 - 3.1.7 Information about NACCC and its Values and National Standards.
 - 3.1.8 Other information as appropriate.
- 3.2 There will be a trial period of 3 months to give the Child Contact Centre and the volunteer time to discover if they are suited to each other. A review will be made midway through the trial period and also at the end.

4. Expenses

- 4.1 We value our volunteers and want to ensure that there are no barriers to volunteer involvement. Out-of-pocket expenses, if required, will be reimbursed for travel and meals only. In order to claim expenses, an expenses form must be completed and given to the Contact Centre Coordinator.

5. Support

- 5.1 The Coordinator, team leaders and other volunteers will offer support to the volunteers. There will be a briefing session at the beginning and a de-briefing at the end of each Child Contact Centre session.
- 5.2 The Coordinator will support all volunteers and will have regular meetings with the volunteers to discuss any problems or issues that may arise.
- 5.3 The Coordinator will receive support and regular supervision sessions from the Chair of the Management Committee (or from another named committee member).

6. Insurance

6.1 The Child Contact Centre has a valid insurance policy which you are advised to read.

7. Confidentiality

7.1 The contact process requires an explicit confidentiality policy, which all Centre workers, which includes Management Committee, volunteers and staff, are obliged to observe.

8. Resolving problems

8.1 The relationship between the Child Contact Centre and its volunteer workers is entirely voluntary and does not imply any contract. However, it is important that the Child Contact Centre is able to maintain its agreed standards of service to the children, families and referrers who use it, and it is also important that volunteers should enjoy making their contribution to this service.

8.2 If your role as a volunteer does not meet with the Child Contact Centre's standards, here is how it will be dealt with:

8.2.1 Initially with a meeting with the coordinator who will explain the concerns.

8.2.2 If this does not resolve the concern then a meeting with the Chair of the Management Committee will be convened.

8.2.3 If your work still does not meet with our standards then we shall have to stop using your services.

8.2.4 At all times you will be able to freely state your case and can have a friend to accompany you.

8.2.5 If you are dissatisfied with any aspect of your work you should:

8.2.5.1 Initially explain your dissatisfaction with the Team Leader

8.2.5.2 If that does not resolve the concern then a meeting with the Co-ordinator should be convened

8.2.5.3 If that does not resolve the issue then a formal meeting with the Chair of the Management Committee should follow.

8.2.5.4 If after this, your dissatisfaction remains unresolved, and we are unable to resolve your grievance, then it would be inappropriate for you to continue to be a volunteer.

8.2.6 At all times you will be able to state your case and can have a friend to accompany you.

8.2.7 This Volunteer policy is freely accessible to all. It will be reviewed on a yearly basis to adapt or improve it.

C. Volunteer Profile

1. Child Contact Centre volunteers should be:
 - 1.1 Cheerful but not artificial;
 - 1.2 Assertive but not dominant;
 - 1.3 Re-assuring;
 - 1.4 Able to understand issues that affect separating families;
 - 1.5 Able to build relationships whilst remaining impartial;
 - 1.6 Able to deal with difficult situations and parents under stress;
 - 1.7 Prepared to work as part of team where people exchange information and support one another;
 - 1.8 Aware of and prepared to follow any policies or guidelines the Child Contact Centre has in relation to Confidentiality, Child Protection, Equal Opportunities etc.;
 - 1.9 Prepared to attend and participate in any training events either at the Child Contact Centre or regionally or nationally.

D. Basic Tasks for a Volunteer

1. These are:
 - 1.1 Helping prepare the Child Contact Centre in advance of people arriving.
 - 1.2 Welcoming Child Contact Centre visitors.
 - 1.3 Registering Child Contact Centre visitors.
 - 1.4 Acting as a host who:
 - 1.4.1 Explains the use of the facilities;
 - 1.4.2 Provides toys;
 - 1.4.3 Provides refreshments.
 - 1.5 Where appropriate:
 - 1.5.1 Talking to, listening to and relaxing Child Contact Centre visitors;
 - 1.5.2 Talking to, playing with and relaxing children;
 - 1.5.3 Helping parents play with their children;
 - 1.5.4 Keeping a watchful eye throughout the contact rooms;
 - 1.6 Tidying up once the Child Contact Centre has closed.

E. New Child Contact Centres and New Workers

1. NACCC's National Standards stipulate that:
 - 1.1 All new volunteers must complete an application form;
 - 1.2 All new volunteers must be interviewed;
 - 1.3 Two references must be obtained for all new volunteers before starting work in a Child Contact Centre;
 - 1.4 All new volunteers must have an enhanced criminal records check through the Criminal Records Bureau before starting work in a Child Contact Centre;
 - 1.5 All Child Contact Centre volunteers must receive induction training before starting work in a Centre. In new Centres this must be provided by NACCC staff or experienced volunteers/workers from established NACCC Member Centres. This training can be undertaken in either a group setting or through a mentoring process with an experienced person;
 - 1.6 All new volunteers in existing Child Contact Centres should have an experienced volunteer as a mentor;
 - 1.7 All new volunteers must complete a probationary period of not less than three months before their appointment is confirmed.

F. Training Volunteers and Staff

1. Child Contact Centres need to keep in mind that the NACCC National Standards require that:
 - 1.1 Every volunteer should have a written description of their role and responsibilities within a Child Contact Centre;
 - 1.2 Each volunteer must undertake induction training followed by the NACCC 10 Training Modules over a three year period
 - 1.3 All staff and volunteers must undertake Safeguarding training annually
 - 1.4 A training record must be kept for each member of staff/volunteer, clearly stating the date and title of any training,
2. All CCC Co-ordinators running supported centres must attend the NACCC Co-Ordinator training once every three years. It will equip them in their role to run their centre safely. It will take place on a regional basis over the course of two days. Part of the Co-Ordinator training is designed to enable them to disseminate the training of the modules to their staff and volunteers.

3. Staff/Volunteer Training.

This has been divided into 10 mandatory modules for all volunteers at supported child contact centres. The training will equip them in their valuable role working in a child contact centre. The courses have been developed following feedback from centres on the issues faced by staff working at supported child contact centres.

The 10 NACCC modules are:

- Safeguarding training
- Induction training for new volunteers
- Family breakdown
- Health and Safety risk assessment
- Encouraging positive contact –working with dads
- Conflict management
- Domestic violence and abuse
- Understanding substance misuse – impact on families
- Managing reluctant family members
- Family risk assessment

These will be delivered at regular times throughout the year. An individual training plan will be given to each Volunteer.

3. Some people may have unhappy memories of education and may shy away from training sessions but with encouragement they will not only benefit from it - but they may end up enjoying it too!

G. Supporting Volunteers

1. NACCC's National Standards state that "every Child Contact Centre must have an agreed system for offering support to its volunteers and staff".
2. Apart from providing training for volunteers it is recommended that Child Contact Centres hold short meetings for their volunteers in advance of and after contact sessions. These meetings mean volunteers will know about families who will be visiting their Child Contact Centre and have the opportunity to talk about anything which may have caused them concern during a contact session.
3. It is also good practice to:
 - 3.1 write to new volunteers confirming their appointment;
 - 3.2 keep the whole volunteer team up-dated with details of their new colleagues;
 - 3.3 Ask at annual intervals whether volunteers wish to continue their commitment.
4. It is important that the Coordinator, team leaders and other volunteers offer their support to each other. The Coordinator or team leaders will supervise all volunteers and have regular meetings with them to discuss any problems or issues that arise. This is also a good opportunity for the Coordinator to thank the volunteer for their contribution.
5. In June every year there is a national 'volunteer's week'. This is a major event involving a wide range of organizations, to recognize the UK's 21 million volunteers. It is a chance to say 'thank you' to volunteers or to use the event to recruit new volunteers.

H. Policy Statement on the Recruitment of Ex-offenders

1. It is a requirement of the DBS' Code of Practice that all Registered Bodies and organisations using their service must treat Disclosure applicants who have a criminal record fairly and do not discriminate because of a conviction or other information revealed. It also obliges organisations to have a written policy on the recruitment of ex-offenders; a copy of which can be given to Disclosure applicants at the outset of the recruitment process.

POLICY

- 1.1 As an organisation using the Disclosure and Barring Service ("DBS") to assess applicants' suitability for positions of trust, Milton Keynes Children's Contact Centre complies fully with the DBS Code of Practice and undertakes to treat all applicants for positions fairly. It undertakes not to discriminate unfairly against any subject of a Disclosure on the basis of a conviction or other information revealed.
- 1.2 Milton Keynes Children's Contact Centres committed to the fair treatment of its staff, potential staff or users of its services, regardless of race, gender, religion, sexual orientation, responsibilities for dependents, age, physical/mental disability or offending background.
- 1.3 We actively promote equality of opportunity for all with the right mix of talent, skills and potential and welcome applications from a wide range of candidates, including those with criminal records. We select all candidates for interview based on their skills, qualifications and experience.
- 1.4 A Disclosure is only requested after a thorough risk assessment has indicated that one is both proportionate and relevant to the position concerned. Within organisations that work directly with children staff require an Enhanced Disclosure and all application forms, job adverts and recruitment briefs will contain a statement that a Disclosure will be requested in the event of the individual being offered the position.
- 1.5 An Enhanced Disclosure asks questions about an entire criminal record.
- 1.6 Where a Disclosure is to form part of the recruitment process, we encourage all applicants called for interview to provide details of their criminal record at an early stage in the application process. We request that this information is sent under separate, confidential cover, to a designated person within Milton Keynes Children's Contact Centre and we guarantee that this information will only be seen by those who need to see it as part of the recruitment process.
- 1.7 We ensure that all those in Milton Keynes Children's Contact Centre who are involved in the recruitment process have been suitably trained to identify and assess the relevance and circumstances of offences. We also ensure that they have received appropriate guidance and training in the relevant legislation relating to the employment of ex-offenders, e.g. the Rehabilitation of Offenders Act 1974.
- 1.8 At interview, or in a separate discussion, we ensure that an open and measured discussion takes place on the subject of any offences or other matter that might be relevant to the position. Failure to reveal information that is directly relevant to the position sought could lead to withdrawal of an offer of employment.
- 1.9 We make every subject of a DBS Disclosure aware of the existence of the DBS Code of Practice and make a copy available on request.
- 1.10 Having a criminal record will not necessarily bar an individual from working with us. This will depend on the nature of the position and the circumstances and background of the offences. This Child Contact Centre recognises that an offence listed in a disclosure is not necessarily a bar to employment.
- 1.11 Milton Keynes Children's Contact Centre will review any information listed in a disclosure and in accordance with the DBS Code of Practice will consider the following when reviewing an applicant's suitability:
 - a. Whether the conviction or other matter revealed is relevant to the position in question,

- b. The seriousness of any offence or other matter revealed,
 - c. The length of time since the offence or other matter occurred,
 - d. Whether the applicant has a pattern of offending behaviour or other relevant matters,
and
 - e. The circumstances surrounding the offence and the explanation(s) offered by the convicted person.
2. The Management Committee or person with legal responsibility will have the final decision as to the suitability of an appointment of a person whose application is subject to disclosure information. This decision will be taken in accordance with the Rehabilitation of Offenders Act 1974 and will be after discussion with the individual applicant

I. Grievance Procedure for volunteers

- 1 There may be occasions when you have a problem relating to your voluntary position, which could have an adverse effect on your performance and attitude unless resolved.
- 2 Should this situation arise, it is hoped that this can be resolved on an informal level between you and the person concerned. If the matter cannot be resolved in this way then you should follow the Organisation's procedure below, which has been designed to settle grievances as quickly as possible.
- 3 All grievances will be dealt with as speedily as possible. At every stage the volunteer will have the opportunity to state their case, accompanied by a supporter of their choice.
- 4 If the grievance is with the volunteer's manager, it shall be referred to the Management Committee.
- 5 The employee should raise the grievance in writing to the person to whom she/he normally reports. A meeting will be arranged to discuss the grievance as soon as possible, not less than 10 working days from when it was raised.
- 6 All requests for consideration under the grievance procedure must be in writing. Notes of discussions held will be made. A copy of these notes will be given to the parties concerned.
- 7 If you are dissatisfied with the outcome of the meeting you have the right to appeal in writing, to the Chair of the Management Committee.
- 8 If the matter is not resolved within 10 working days, it will be referred to the Management Committee who will call a meeting within 15 working days.
- 9 If no satisfactory conclusion is reached by this stage, the parties will consider whether conciliation or arbitration is appropriate. The organisation may refer the dispute to ACAS or another mediation agency, whose findings may, by mutual prior agreement, be binding on both parties.

J. Diversity Policy

1. The Diversity Policy for Milton Keynes Children's Contact Centre is firmly committed to diversity in all areas of its work. We believe that we have much to learn and profit from diverse cultures and perspectives and that diversity will make our organisation more effective in meeting the needs of all our community.
2. We are committed to developing and maintaining an organisation in which differing ideals, abilities, backgrounds and needs are fostered and valued and where those with diverse backgrounds and experiences are able to participate and contribute. We will regularly evaluate and monitor our progress towards diversity.
3. We will ensure that all Child Contact Centre users and referrers are aware that we have equal opportunities and diversity policies, which they can see upon request.

K. Equal Opportunities Policy

1. We live in a wide-ranging society where people are discriminated against both intentionally and unintentionally because of their race, skin colour, ethnic origin, religion, cultural beliefs, nationality, national origin, gender, sexuality or age. People suffering from HIV and Aids and people with disabilities may be discriminated against due to lack of understanding about their capabilities and experiences. We recognise that any one may experience discrimination and as we are opposed to this situation, we will take steps to challenge it.
2. The Milton Keynes Child Contact Centre states its intention to work for the furtherance of equal treatment in volunteering, employment, service provision, committee structure and membership.
 - 2.1 Volunteering/employment opportunities are open to all, within the context of our local community. Although the majority of our volunteers are recruited from local service organisations, this does not preclude others from volunteering, especially from underrepresented groups. All volunteers, regardless of whether they are recruited from a service organisation or not, have to follow the same recruitment process. That is, they must complete an application form, supply two referees, abide by NACCC's National Standards for Child Contact Centres, undergo an initial training programme and have a three-month probationary period.
 - 2.2 The aim of our policy is to ensure that no-one receives less favourable treatment on the grounds of race, skin colour, ethnic origin, religion, cultural beliefs, nationality, gender, sexual orientation., age, status or disability.
 - 2.3 We value and respect all individuals using the Child Contact Centre, both families and staff/volunteers. We will aim to ensure that our service provision is appropriate, relevant and accessible to all groups of people represented in the community.
 - 2.4 We will strive to ensure that no member of staff, management committee member, volunteer or any of the families experiences unlawful discrimination.
 - 2.5 Volunteers/staff will exercise thoughtfulness and care to avoid stereotyping of individuals and groups.
 - 2.6 Any racist or other offensive remarks or behaviour will not be tolerated and always challenged
 - 2.7 If you feel you have been discriminated against, please let the Centre Co-ordinator know, who will pro-actively look into and attempt to resolve any concern raised. Should this not be possible then the centres complaints procedure should be used.
 - 2.8 We will ensure that all Child Contact Centre users and referrers are aware of this policy.
 - 2.9 This policy will be annually reviewed and updated if required.

L. Confidentiality Policy

1. The Milton Keynes Child Contact Centre recognises that the contact process requires explicit confidentiality which all Child Contact Centre workers are obliged to observe. Therefore, we will ensure that:
 - 1.1 Volunteers undertake not to discuss or disclose any details relating to a family outside of the Child Contact Centre save where authorised to do so under the centres policies.
 - 1.2 Volunteers do not make verbal or written reports in any family proceedings.
 - 1.3 The dates and times of a family's attendance will be made available to referring agencies or parents upon request and for payment of the appropriate fee (Set from time to time by the management committee). No other information will be released unless a) a child is felt to be at risk of harm either inside or outside of the Child Contact Centre or b) anyone using the Child Contact Centre or a volunteer is at risk from physical violence. In those circumstances, subject to approval from the Management Committee, a brief summary of events will be provided by the Co-Ordinator/volunteer and disseminated to all relevant parties.
 - 1.4 A parent's details such as his/her address and telephone number will not be passed to any other person (including their former partner) or agency without their permission.
 - 1.5 The only exceptions to this will be if a) a child is felt to be at risk of harm or b) anyone using the Child Contact Centre or a volunteer is at risk of physical violence.
 - 1.6 Unless there is an agreement from the Contact Centre which allows them to do otherwise, Solicitors, CAFCASS Officers, Social Workers or any other individual or agency will not be allowed to carry out family assessments on Child Contact Centre premises.
 - 1.7 All potential volunteers must have a DBS Disclosure carried out by the DBS. The results of this Disclosure will be made available to the Coordinator and/or the Management Committee.
 - 1.8 All information relating to families and volunteers will be kept in a secure place at all times.
 - 1.9 All information relating to families and volunteers which has not been used for three years will be treated as confidential waste and disposed of as such, except in the case of the accident book, which will be kept indefinitely.
 - 1.10 Child Contact Centre users, referrers, volunteers and staff will all be aware of the existence of this policy and have access to it upon request.
2. This policy will be reviewed and if necessary updated annually.

M Complaints Policy and Procedure

1. Milton Keynes Child Contact Centre aims to provide families and referrers with the best possible service. However, from time to time there are occasions when users of our service may feel that the quality or level of service provided falls short of what can reasonably be expected. Your continued involvement and goodwill is of great value to us. If you have a complaint, we would like you to tell us about it.
2. The aim of the procedure is to enable any complaints made by a member of a family using the Centre to be resolved quickly, effectively, fairly and in as conciliatory a way as possible.
3. A complaint may be initiated by a parent's legal representative, a parent or a representative of another agency who is involved with the family. All matters relating to this procedure will be conducted in a discreet manner.
4. If the complaint progresses past Stage 1 then the matter will be dealt with by an Investigator, appointed by the Management Committee. The Investigator cannot be a volunteer and will usually be a member of the Management Committee. If the Chair of the Management Committee is not the Investigator he or she will keep the Chair involved of the progress of the complaint.
5. Our complaints procedure should be sent to the parent immediately when it was requested (within 14 days)
6. A complaint will not be considered unless the procedure has been activated within 6 weeks of the incident occurring.
7. Stage One. Complaints should be made initially to the Co-ordinator or Assistant Coordinator. If complaints cannot be satisfactorily resolved there and then, brief written notes of the complaint and the circumstances that led to it should be made and the complainant should sign the notes. These notes should be given to the Coordinator - or Assistant Coordinator if the Coordinator was on duty at the time of the complaint - as soon as possible. They will then investigate the circumstances in so far as the Child Contact Centre is concerned making notes, which should be signed and dated. The Coordinator - or Assistant Coordinator - will then discuss the matter with the complainant and will attempt to resolve the issues to the satisfaction of all concerned
8. In the event that matters are not able to be resolved then the complainant must proceed to Stage Two.
9. Stage Two. The complainant will be invited to submit details in writing within 7 days to the Chair of the Management Committee who will acknowledge receipt of the complaint. An Investigator will be appointed to investigate the complaint and send a full written reply within 30 days, or explain why further time is necessary.
 - 9.1 The reply will:
 - 9.1.1 Set out the complaint so that the complainant can be sure it has been understood.
 - 9.1.2 Describe the event and circumstances surrounding them
 - 9.1.3 Say whether or not the complaint is deemed to be fair, giving reasons for the decision. It should be noted that if such an admission could have legal/insurance implications the Investigator will have taken legal advice or contacted the insurers before writing.
 - 9.1.4 Apologise on behalf of the Child Contact Centre (if the complaint is deemed to be fair) and explain the steps it has taken to avoid it happening again.
 - 9.1.5 Notify the complainant that if he/she is not happy with this decision, then he/she must

notify the Chair of the Management Committee within 14 days of receiving the reply that he/she wishes to take it further to Stage Three.

10. Stage Three. If the complainant wants to have his/her complaint heard at a Management Committee of the Milton Keynes Childrens Contact Centre, he/she will be entitled to bring a friend who can speak for the complainant, as can the person from the Child Contact Centre who is subject of the complaint (if appropriate). Three members of the Management Committee (excluding the Investigator) shall hear the complaint. Both the complainant and the person against whom the complaint has been made shall be allowed to have their say and all previous written notes and the previous investigations shall be taken into account. A written decision will be sent to all involved as is described in paragraph 9 above. If after this procedure has been carried out the complainant is still not happy with the response, they should send a copy of all correspondence to the Chief Executive of NACCC (or representative in his/her absence) so that the NACCC Complaints procedure can be carried out.
11. Recording Complaints
 - a. If the complaint is resolved at Stage 2 or 3 then the matter shall be reported at the next Management Committee Meeting of Milton Keynes Contact Centre and recorded in the minutes of that meeting.
 - b. The written records of all complaints will be held by the Chair of the Management Committee, including any written legal or insurance responses and transferred to his/her successor as a strictly confidential file.

N Domestic Violence and Conflict Management Policy

1. Milton Keynes Child Contact Centre believes that everyone has the right to live safely and without the fear of violence and cruelty. We recognise that domestic violence is unacceptable and that it occurs throughout society, irrespective of class, culture, gender, income, race, religion or sexuality. Its effects are far-reaching and can impact on others, notably the children. We recognise that every child has the right to grow and develop in an environment free of domestic violence, whether directly as a victim or witness of violence in its own home or in the community.
2. Milton Keynes Child Contact Centre accepts that some families using its Centre will have experienced varying levels of domestic violence and we will ensure that they will receive sensitive and appropriate services. We also accept that the Centre needs to be organised and run in a way which allows these families, other Centre users and volunteers/staff to be safe. In order to meet these requirements we will ensure that:
 - 2.1 The Centre's referral form will ask one or more questions about domestic violence.
 - 2.2 No family will be accepted until a referral form has been completed in full and received by the Coordinator.
 - 2.3 Any information concerning domestic violence or the abuse of drugs / alcohol will be treated seriously.
 - 2.4 Use of the Centre will be denied to individuals or families where the coordinator feels their presence is likely to present a threat to the well-being of other Centre users and volunteers/staff.
 - 2.5 Once a family has been accepted the coordinator will consider their needs and develop a means by which they can be met. These will include the following:
 - 2.5.1 Parents being invited to visit the Centre separately in advance of contact commencing.
 - 2.5.2 Parents being given clear instructions in writing about what times to arrive.
 - 2.5.3 Where appropriate, resident parents being asked to explore the possibility of someone other than themselves or their new partner bringing the child(ren) to the Centre.
 - 2.5.4 The contact waiting room doors being kept closed and precautions taken to ensure parents do not visit the refreshment area or toilets at the same time.
 - 2.5.5 Asking one parent to wait at the end of contact until the other has left the Centre and the area immediately around it.
 - 2.5.6 Ensuring that addresses, telephone numbers and other sensitive information always remain strictly confidential.
 - 2.6 Any distress to children or adults brought about by bullying or pressure to disclose information will be dealt with promptly and firmly.
 - 2.7 If an individual or family's behaviour is threatening, causes distress or is disruptive they will be asked to leave. See the exclusion policy detailed at Q below.
 - 2.8 If an individual or family refuses to leave the police will be called.

O Essential Requirements for Volunteers and Staff in Relation to Managing Domestic Violence and Conflict

1. There will be a minimum of three volunteers/staff on duty at all times and this number will increase depending upon the number of families using the Centre and rooms to be covered.
2. Volunteers/staff will be made aware of the particular needs of each family attending the Centre.
3. All volunteers/staff will receive training in the areas of domestic violence, child protection and conflict management.
4. Volunteers/staff will have immediate access to a telephone when the Centre is open.
5. The Centre will have an agreed procedure to follow in the event of an incident or an emergency. All volunteers/staff will be made aware of this.
6. The Centre will have a recognised and easily accessible system for offering support to volunteers/staff who have become involved in stressful or violent incidents.
7. Additional Requirements
 - 7.1 Referrers and families using the Centre will be made aware of its policy in relation to domestic violence.
 - 7.2 Any individual or agency wishing to challenge how the Centre is implementing its policy in relation to domestic violence should be referred to the Centre's complaints procedure.
 - 7.3 The Centre's policy in relation to domestic violence will be reviewed and if necessary updated annually.
 - 7.4 Action to be taken when conflict arises:-
 - Make sure all the children are safe and out of the way
 - Move those involved to a quiet area if possible
 - Never back them into a corner, either physically or psychologically
 - Remain polite and respectful and never lose your temper
 - Keep the tone of your voice down and lower than the person who is angry
 - Never tell them to "calm down"

P Photograph Policy

1. Due to the possible abuse of photographs (digital or otherwise) or other images of children the contact centre has had to develop and apply a policy for the taking of photographs etc.
2. A photograph may not only have your own child as a subject but also other children who for many reasons perhaps should not be in the image.
3. While the centre appreciates how important and precious photographs of one's children are as they are growing up it is hoped you will understand and abide by the rules that have to be set down. They are for the benefit of all the users of the centre and not designed to restrict your enjoyment of contact with your child or children
4. As a consequence we shall insist that every user of the contact centre and on every referral from now on the following rules shall apply:
 - 4.1 No camera, or similar equipment shall be allowed on or be used in the contact centre without 14 days prior notice of a request in writing to Contact Centre Coordinator either by e-mail or by post to the address at the front of the Policies and procedures. While any such request will be treated sympathetically, only when such a request has been approved in writing by the Coordinator can the camera be used.
 - 4.2 No camcorders, cine cameras, video recorders or other similar devices will be allowed into the centre under any circumstances.
 - 4.3 No mobile phone capable of being used for taking photographs or making video recordings should be visible at any time in the centre unless prior written approval has been requested.
 - 4.4 When giving notice of such an intention the written consent of the resident parent or those persons with parental responsibility must accompany the request.
 - 4.5 Any request, even with consent, must not contravene any court order relating to the child.
 - 4.6 Any photograph or other image taken in compliance with these rules must not in any circumstances whatsoever contain any image of any child or children at the Centre other than those for whom written consent has been obtained.
 - 4.7 While the number of photographs will not be limited by the Centre it is requested that all users of the Centre abide by any reasonable request from the volunteers or staff of the Centre or the use of the equipment will be immediately forbidden.
 - 4.8 The Contact Centre reserves the right to refuse the use or continued use of any photographic equipment without notice if in the opinion of the volunteers or staff of the Centre such use affects the smooth running of the Centre.

Q Exclusion Policy

1. The trustees, committee, staff and volunteers of the Contact Centre regret having to initiate an exclusion policy in relation to parents and others who abuse the use of the contact centre or any member of staff or volunteer or cause any disruption.
2. Unfortunately, it has proved necessary to introduce such a policy but please be assured it will be a remedy of last resort. If exclusion can be avoided by any other reasonable solution any alternative will be given every consideration.
3. The smooth running of the Contact Centre is first and foremost for the benefit of all the children who use it. Disruption or inappropriate behaviour cannot be tolerated. Any person who behaves in such a way or threatens the relative calm of the contact centre will be at risk of exclusion.
4. Any member of staff or volunteer may exclude any person from the Contact Centre.
5. If anyone is excluded they must leave the premises immediately and not return until and unless the exclusion is lifted. If they fail to leave the police will be called to assist.
6. In the event of an exclusion the parties to the referral will be notified as soon as possible. It is a matter for the parties' what action to then take concerning continuation of contact in particular if contact is pursuant to a Court Order but once excluded the family shall not be entitled to return to the Contact Centre and a place will no longer be available at our Centre.
7. The Contact Centre has been informed by the Family Court at Milton Keynes that on confirmation from either party that there has been an exclusion in relation to any order it makes the court will list the case a directions appointment as soon as possible so that the welfare of any child affected by the exclusion can be considered as soon as possible.
8. The staff and volunteers will not give evidence for either parent or the child in relation to any exclusion unless summoned by the court to do so. A letter may be prepared by the Trustees on request of any party setting out why there was an exclusion, subject to the discretion of the Trustees.
9. It is noted that the Contact Centre often has high demand. In order to ensure that we are meeting the needs of as many families as possible in the Milton Keynes area please note that the Contact Centre operates a "three strikes policy" as detailed on the referral form. If any family miss three consecutive sessions (without prior agreement from the contact centre co-ordinator) their place will be removed and shall be given to another family. The family shall be warned after 2 missed sessions of the consequences and following 3 missed sessions the place shall be removed. Exclusion in those circumstances does not prevent a further referral being made should the place still be required but this will be subject to a) a further admin fee for the referral and b) the contact centre's discretion as to whether the referral is accepted. The Contact Centre Co-Ordinators decision is final as to whether to accept a referral.

R. Exclusion Policy Procedure

1. The paramount principle is the welfare of the child. With that in mind it is hoped that rarely, if ever, will a member of the staff or volunteer of the Contact Centre have to exclude anyone from the centre during a contact period.
2. It is for the welfare of the children, all of the children not just one or two children involved in any incident that we must not be afraid to exercise exclusionary power if no other remedy is appropriate and all other avenues have been explored or considered.
3. The exclusion policy is set out in a Section Q of the Policies and Procedures. This procedural note is for the benefit of staff and volunteers who exclude a person from the Contact Centre.
4. It is impossible to set out all the circumstances in which a person may have to be excluded from the Contact Centre. A guide might be if a person's behaviour, attitude or the behaviour, or attitude of any person accompanying them is such that it affects the smooth running of the Contact Centre.
5. Exclusion should be a remedy of last resort. Please ensure that all other methods of persuasion or compromise are attempted before exclusion.

6. Exclusion Procedure

- 6.1 In the event of exclusion due to a family missing three consecutive sessions the Co-Ordinator should warn the family after 2 missed sessions of the consequences and if they fail to attend for a third session the Co-Ordinator need only notify all parties to the referral that their place has been removed and to use the centre again will require a further referral.
- 6.2 In the event of exclusion due to behaviour or any other reason save for missing three consecutive sessions then the procedure to be followed is:-
- 6.3 Tell the person or persons involved exactly what behaviour it is that is inappropriate and ask them to desist.
- 6.4 Give the person or persons involved clear warning that if their inappropriate behaviour continues they will be excluded.
- 6.5 To exclude someone you need only tell them that they are excluded from the Contact Centre and that they must leave immediately or you will call the police. If they do not leave immediately CALL THE POLICE. A THREAT NOT CARRIED THROUGH IS WORTHLESS.
- 6.6 Once the person has left the premises make an immediate note of the incident. Sign it and date it. Ensure that the name and address of the person or persons excluded is made known to the Contact Centre Coordinator immediately.
- 6.7 The Coordinator must inform the Chairman of the Trustees (or such other person as may be agreed by the committee) of the details of the exclusion as soon as possible and within 7 days of any incident and, if possible, provide a copy of the note made by the excluder.

S Health and Safety Policy

1. STATEMENT OF INTENT

- 1.1 Milton Keynes Children's Contact Centre is committed to ensure the health, safety and welfare of its volunteers/staff and other persons who may be affected by our activities. We shall ensure that the requirements of the Health and Safety at Work etc. Act 1974 and other relevant statutory provisions are carried out so far as reasonably practicable. In particular we will so far as reasonably practicable, provide:
- 1.1.1 Premises which are well maintained in a safe condition.
 - 1.1.2 Environments that are safe and without risk to health.
 - 1.1.3 Equipment and systems of work that are safe and without risk to health.
 - 1.1.4 Arrangements to identify and assess/minimise risk to volunteers/staff and others who may be affected by our activities.
 - 1.1.5 Sufficient information, instruction, training and supervision to ensure the health and safety of volunteers/staff and others who may be affected by our activities.
 - 1.1.6 Adequate facilities and arrangements to enable volunteers and staff to be consulted on any matter relating to their health, safety and welfare whilst at work.
 - 1.1.7 The implementation of this policy will be regularly monitored to ensure that the objectives are being achieved. The policy will also be reviewed and if necessary revised to reflect any changes in organisational or legislative requirements.

2. ORGANISATION

- 2.1 Ultimate responsibility for health and safety lies with the Contact Centre Coordinator who will ensure that adequate resources are made available to achieve the aims set out in this policy statement.
- 2.2 The person responsible for the co-ordination of Health & Safety matters is the Contact Centre Coordinator.
- 2.3 The successful implementation of this policy requires total commitment from all volunteers/staff within the organisation. Each individual has a legal obligation to take reasonable care of his or her own health and safety, and the safety of other people who may be affected by his or her acts or omissions.
- 2.4 Line of Reporting



2.5 Health & Safety Responsibilities

- 2.5.1 Management Committee (or Overseeing Organisation)
 - 2.5.1.1 Ensuring that this Health & Safety policy is followed by all staff/volunteers.
 - 2.5.1.2 Approving any action recommended by risk assessments undertaken by the Centre Coordinator or Safety Officer.
 - 2.5.1.3 Investigating any accidents with Centre Co-ordinator/Safety Officer that have been reported under RIDDOR (Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995).
- 2.5.2 Centre Coordinator/Safety Officer
 - 2.5.2.1 Coordinating Health & Safety matters for the Organisation.
 - 2.5.2.2 Ensuring this policy is put into practice at the Centre.
 - 2.5.2.3 Carrying out a fire risk assessment and emergency procedures.
 - 2.5.2.4 Carrying out risk assessments as appropriate including an assessment into the risk associated with pushing and pulling of loads.

- 2.5.2.5 Reporting the findings of all risk assessments to the Management Committee /Overseeing Organisation who will also approve any action required to remove or control risks.
- 2.5.2.6 Ensuring the action required is implemented and that these actions have removed or reduced the risks.
- 2.5.2.7 Carrying out periodic formal active monitoring to check workplace precautions continue to work effectively.
- 2.5.2.8 Reviewing risk assessments annually or when the work activity changes, whichever is soonest.
- 2.5.2.9 Identifying all machinery and equipment needing maintenance;
- 2.5.2.10 Ensuring effective maintenance procedures are drawn up and are implemented;
- 2.5.2.11 Ensuring that all identified maintenance is implemented.
- 2.5.2.12 Checking that new machinery and equipment meets health and safety standards before it is purchased.
- 2.5.2.13 Checking that new chemicals or substances can be used safely before they are purchased.
- 2.5.2.14 Identifying all chemicals or substances that are a hazard and would require a risk assessment.
- 2.5.2.15 Recording all accidents, incidents, near misses and cases of work-related ill health in the accident book and for reporting accidents under RIDDOR - another staff member should be nominated for this in the absence of this person.
- 2.5.2.16 Investigating accidents, incidents, near misses and cases of work- related ill health for the Organisation following the investigation procedure and will act on findings to prevent a recurrence.
- 2.5.2.17 providing induction training for staff and consulting with staff on Health & Safety issues -this could be via an agenda item at staff meetings.
- 2.5.3 All Centre staff/volunteers (including the staff mentioned above)
- 2.5.3.1 Co-operating with supervisors on health and safety matters.
- 2.5.3.2 Not interfering with anything provided to safeguard their health and safety.
- 2.5.3.3 Taking reasonable care of their own health and safety, complying with any rules or regulations in place and any safe systems of work.
- 2.5.3.4 Using equipment in accordance with instructions and training provided, not intentionally damaging or recklessly interfering with anything provided for the health and safety of themselves or others
- 2.5.3.5 Check that workplace precautions continue to work effectively to reduce risk.
- 2.5.3.6 Reporting on all health and safety concerns to the Centre Co-ordinator, Safety Officer or Management Committee as appropriate.
- 2.5.3.7 Reporting any accidents, incidents, near misses and cases of work-related ill health to the Centre Coordinator/Safety Officer or alternative staff member if the nominated person is not available.
- 2.5.3.8 Following regulations regarding security.
- 2.5.3.9 Ensuring that any visitors and users of the Centre are made aware of emergency procedures and are supervised during an emergency evacuation.
- 2.5.3.10 Undertaking training as required.

Any volunteers/staff failing to comply with these principles will be subject to disciplinary action, which could lead to dismissal.

C. ARRANGEMENTS

- 1. Emergencies
 - 1.1 Fire and evacuation
 - 1.1.1 The Centre Coordinator/Safety Officer is responsible for ensuring that a fire risk assessment is undertaken and implemented for the Organisation. There is a fire procedure which all staff,

volunteers and users of the Centre are made aware of, which takes into consideration the sensitive nature of a Contact session.

- 1.1.2 Emergency evacuation will be tested every 12 months. This is the responsibility of the Centre Coordinator/Safety Officer.
- 1.1.3 In the event of a fire, fire extinguishers should only be operated by a staff member who has been trained in their correct use.
- 1.1.4 Staff / Volunteers must acquaint themselves with the locations of both Fire exits and Fire alarm points.
- 1.1.5 Staff / Volunteers must participate in any fire drill.
- 1.2 Bomb alert
 - 1.2.1 The Centre Coordinator is responsible for ensuring that a bomb alert risk assessment is undertaken and implemented for the Centre. This may involve setting an assembly point 100 metres from the Centre and opening all windows before evacuation.
- 1.3 Security of Staff/Volunteers and Centre users
 - 1.3.1 The Centre Coordinator/Safety Officer is responsible for ensuring that a security risk assessment is undertaken and implemented for the Centre staff / Volunteers and Centre users.
 - 1.3.2 The last person to leave the premises must ensure that the windows are closed, appliances and lights are switched off and doors are locked. Staff should request identification from any visitor that they do not recognise and appears suspicious and should call the police if unsure.

2. Accidents

- 2.1 A First Aid box must be kept at the Centre. It will contain:
 - Assorted sterile adhesive dressings (piasters).
 - Medium sterile dressings.
 - Large sterile dressings.
 - Sterile eye pads.
 - Triangular bandages.
 - Safety pins.
 - Disposable gloves.
 - Advice leaflet.
- 2.2 Remember that there is no definitive list and each kit should reflect what it would be used for. For example, ensure that you have some small dressings and plasters if there is the possibility of using it for children.

© EMERGENCY AID Reference Guide (St John Ambulance)

All accidents, incidents, near misses and cases of work-related ill health at any site are to be reported to the Centre Co-ordinator (or nominated person in the absence of the Centre Coordinator) and recorded in the accident book that is kept with the first aid box. The Centre Coordinator or other nominated person is responsible by law for reporting serious accidents, diseases and dangerous occurrences under RIDDOR.

(See the Health and Safety Responsibilities section for duties relating to the investigation of accidents).

Signed..... Date
 Position.....

This Health and Safety policy is reviewed annually, but is in any event updated whenever considered necessary.

T Child Protection / Safeguarding Children Policy

Introduction

1. Milton Keynes Child Contact Centre believes that all children have the right to be protected at all times and that the welfare of the child is paramount. It recognises that child abuse occurs in all religions, all cultures and all social classes. Confidentiality issues will be overridden by the need to act for the welfare of the child. All children have the right to be safe and not to be hurt. For us to do the right thing in an emergency we need to:-
 - Be familiar with our policies
 - Have discussions between the volunteers and Co-Ordinator before any action is taken if possible
 - If there is any doubt about what to do, telephone the NACCC helpline: 07540 703577. It is open every Saturday 10am-6pm. It is a dedicated phone line run by NACCC's Regional Support Managers to help you safeguard everybody using or working in contact centres.

BASIC PRINCIPLES

2. Responsibility for a child or children using Milton Keynes' Children's Contact Centre always rests with their parents and not volunteers. Nevertheless, every volunteer is responsible for:
 - 2.1 preventing the physical, sexual and emotional abuse of children whilst using their Child Contact Centre;
 - 2.2 listening to concerns expressed by parents or children and advising them how to report any abuse;
 - 2.3 reporting abuse themselves in certain circumstances.
3. Where there is an allegation of or suspected child abuse the interests and safety of the child/children involved must always come first. This means that if there is a conflict of interest between parent and a child, the interests of the child should always be put first.
4. Milton Keynes Childrens Contact Centre will ensure that:
 - 4.1 Child Contact Centre users and referrers are aware that the Child Contact Centre has a Child Protection/Safeguarding Children Policy they can see upon request.
 - 4.2 All staff/volunteers have an understanding of what constitutes child abuse and procedures that need to be followed to report or prevent it.
 - 4.3 There is a recognised procedure for Child Contact Centre volunteers/staff to report allegations of or suspected child abuse.
 - 4.4 Child Contact Centres providing Supported Contact will not knowingly accept a referral when somebody involved has been convicted of any offence relating to a) physical or b) sexual abuse of any child, unless there are exceptional circumstances and they have sought appropriate professional advice.

Recruitment

- 4.5 The risk of staff/volunteers being potential, actual or convicted perpetrators is reduced by one or a combination of the following prior to their appointment:
 - 4.6.1 The completion of an application form.
 - 4.6.2 An interview.
 - 4.6.3 Obtaining references from two people who have first-hand knowledge of them.
 - 4.6.4 Carrying out a DBS.
 - 4.6.5 Making any appointment conditional on the successful completion of a probationary period.
- 4.7 Staff and volunteers are aware that in most situations parents should accompany children to the toilet. If there has been a request for a staff/volunteer to take a child to the toilet, or there is concern about a parent, they should be accompanied by another worker. Neither staff nor volunteers should take children to the toilet on their own.
- 4.8 There is an easily accessible and on-going support structure available to staff and volunteers who have to deal with a family where there has been alleged or actual child abuse.

Accountability

5. A copy of this policy will be given to all volunteers at Milton Keynes Children's contact centre and shall be made available on their website.

Managing safeguarding and promoting the welfare of children within MKCCC

- 6 Milton Keynes Child Contact Centre will have one named member of staff who will be responsible for ensuring that the Policy and its processes are implemented and adhered to. This person is: the Co-Ordinator. The Management Committee who also ensure adherence to safeguarding policies

Education and Training

7. Milton Keynes Children's Contact Centre induction process will include "Safeguarding and promoting the welfare of children" training for all volunteers. This is mandatory. Records of all training will be kept by the Co-Ordinator. Training will be updated on annual basis. Volunteers will have access to the Co-Ordinator or Management Committee or the NACCC safeguarding team in the event of any concerns.

- 7.1 Prior to any formal training all volunteers have an induction session with the Co-Ordinator at which they are made aware of the importance of adhering to the Milton Keynes Children's Contact Centre that no volunteer should at any time be in an isolated situation with any of the children using our Centre. The purpose of this policy is three-fold:

- To ensure that at no time a child is left in a vulnerable situation alone with any individual associated with the contact centre;
- To ensure that at no time a volunteer is vulnerable to unfounded accusations of unacceptable or even abusive behaviour towards any child using our facilities
- To ensure that volunteers are alert to the possible abuse of any child using our centre. All volunteers are made aware of the Child Protection Policy and of what constitutes child abuse as an integral part of their induction training. Volunteers are made aware that although all child remain the responsibility of their parent or the adult that is involved at contact at all times, the volunteers are responsible for:-
 - Listening to any concerns raised by the parents or carers of the children and advising them on how to report any actual or alleged abuse;
 - Discussing any apparent abuse with the Co-Ordinator and reporting any such incidents.

Allegations or suspicions of abuse.

8. Making a decision whether or not to report one's worries to Social Services is not made easier by the context in which the children are seen. The child may be very anxious about seeing the other parent or some of the parent with whom the child lives anxiety may affect the child.
9. Suspicions of abuse are very difficult to handle. If anyone has worries they should be discussed with the Co-Ordinator or the rest of the team. Child abuse may take many different forms – neglect, emotional abuse, physical abuse and sexual abuse. More than one of these may occur at the same time. Principles to guide this work
 - Always be alert for signs of abuse and neglect. It can happen anywhere
 - All those involved in child protection cases, including children, families and individuals alleged to have been responsible for harm or neglect, must be treated with respect.
 - Do not discuss the subject with a suspected abuser
 - The welfare of the child over-rides our confidentiality policy where abuse is suspected
 - Be familiar with the checklist
 - Speak with the Co-Ordinator or telephone the NACCC helpline if appropriate
 - If an adult has made allegations, tell them that you are going to pass on that information to the professional agencies: if possible, encourage the person who has made the disclosure to report it themselves
 - Never attempt to apportion blame

- Do not try to “go it alone”. Children are best protected when all agencies work together.
 - Avoid being used by a parent who is assembling evidence for a family law hearing.
- Allegations may arise from parents, or by a child or by suspicions of one of the volunteers. The latter is difficult to handle, but in all cases remember the welfare of the child is paramount.

Concerns by volunteers

If a volunteer is concerned that there may be abuse, they should write a clear note of what was seen or they have been told (use only initials of names involved); what the concerns were and inform the Co-Ordinator immediately. All notes/actions should be clearly documented signed and dated. Ask the other volunteers who heard/witnessed the incident to either sign it or write a note themselves.

Keep a copy of the note you have written and send a copy to the Co-Ordinator. If you have any doubt as to the procedures to follow ring the NACCC helpline on 07540 703577.

Allegations by parents

If one of the parents alleges their child is being abused by anyone immediately involve the Co-Ordinator. Write down fully what they say. Ask whether it has been reported. If they haven't reported it, it may be appropriate to ask them why they haven't, because some time would have passed since the incident would have occurred. If they haven't reported it, it could be that this is a false allegation, however you should not take this any less seriously.

Advise them that they have a duty to report it to the appropriate authority and tell them that we will consider what action to take. If it is alleged that a child has suffered significant harm or is at imminent risk it is our duty to inform the Children's Services Department (their emergency number is at the beginning of this Policy).

If we consider the child to be in immediate danger, we should inform the Police. The probability is that they have made the allegations to a number of people already. In which case record what has been said and inform the Co-Ordinator. It may be appropriate to inform the solicitor of the person who made the allegation in writing.

Response to disclosure or an allegation by a child.

A child's verbal allegations must always be treated with the utmost respect. Children are entitled to be listened to and to have their allegations treated seriously. Remember the child will have spoken to you because they feel they can trust you. Be prepared to respond calmly. Children are more likely to allow you to help if they know that you are prepared to listen and to take what they are saying seriously.

They may be frightened. They may have been threatened or told to keep “secrets” Explain that you need to involve another volunteer (you need to do this in case the child is later “persuaded” to deny making the allegations) but tell the child that you trust the other volunteer. Ideally involve the Co-Ordinator as the other volunteer.

What to do when child abuse has either been disclosed or alleged.

Act immediately but:

- Remain calm, sensitive and focussed;
- Take whatever steps are necessary to ensure the safety of the child/children involved
- Involve the co-ordinator/team leader and other volunteers at the earliest opportunity
- Contact the Police immediately if you feel that a child is at risk of harm once they leave the centre
- Listen carefully to what the child(ren) or adult(s) are telling you. Offer respect, kindness and comfort. Say they were right and brave to tell;
- As the responsibility for investigating child abuse rests with the local Social Services department and it may jeopardise their enquiries, do not ask the child or adult any leading or searching questions;
- Do not promise “never to tell”

- Write down what the child(ren) or adult(s) making the allegations is telling you. Only record the facts and avoid including personal opinions or judgments
- Report what has been said along with the names and addresses of the adults/children involved to your local Social Services department immediately. To make it easier to report any concerns there is a form for you to use – available from the Co-Ordinator
- Whatever they say or do make sure that the child(rens) welfare remains paramount
- Do not be afraid to share your feelings with somebody else and ask for help if the process of dealing with the actual or alleged child abuse upsets you or distresses you

Review of Safeguarding and Child Protection Policy

10. This will take place annually. Additional changes to take account of new legislation and practice directions will also be made as and when required. Copies of the revised policy will be made available to Milton Keynes Children's Contact Centre management committee, trustees and volunteers.

U Policy Statement: Data Protection Policy

1. It is a requirement of the DBS's Code of Practice that all Registered Bodies must have a written policy on the correct handling and safekeeping of Disclosure information. It also obliges Registered Bodies to ensure that a body or individual, on whose behalf they are countersigning Disclosure applications, has a written policy.

2. General Principles

2.1 As an organisation using the Disclosure and Barring service ("DBS" to help assess the suitability of applicants for positions of trust, Milton Keynes Children's Contact Centre complies fully with the DBS Code of Practice regarding the correct handling, use, storage, retention and disposal of Disclosures and Disclosure information. It also complies fully with its obligations under the Data Protection Act 1998 and other relevant legislation pertaining to the safe handling, use, storage, retention and disposal of Disclosure information and has a written policy on these matters, which is available to those who wish to see it on request.

3. Storage and Access

3.1 Disclosure information should be kept securely, in lockable, non-portable, storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties.

4. Handling

4.1 In accordance with section 124 of the Police Act 1997, Disclosure information is only passed to those who are authorised to receive it in the course of their duties. We maintain a record of all those to whom Disclosures or Disclosure information has been revealed and it is a criminal offence to pass this information to anyone who is not entitled to receive it.

5. Usage

5.1 Disclosure information is only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

6. Retention

6.1 Once a recruitment (or other relevant) decision has been made, we do not keep Disclosure information for any longer than is necessary. This is generally for a period of up to six months, to allow for the consideration and resolution of any disputes or complaints. If, in very exceptional circumstances, it is considered necessary to keep Disclosure information for longer than six months, we will consult the DBS about this and will give full consideration to the data protection and human rights of the individual before doing so. Throughout this time, the usual conditions regarding the safe storage and strictly controlled access will prevail.

7. Disposal of Disclosure Information

Once the retention period has elapsed, we will ensure that any Disclosure information is immediately destroyed by secure means, i.e. by shredding, pulping or burning. While awaiting destruction, Disclosure information will not be kept in any insecure receptacle (e.g. waste bin or confidential waste sack). We will not keep any photocopy or other image of the Disclosure or any copy or representation of the contents of a Disclosure. However, notwithstanding the above, we may keep a record of the date of issue of a Disclosure, the name of the subject, the type of Disclosure requested, the position for which the Disclosure was requested, the unique reference number of the Disclosure and the details of the recruitment decision taken.

V. Policy for Disclosure & Barring Service (“DBS Policy”)

General Principles

1. It is a requirement of any new volunteer or contractor/employee of Milton Keynes Children’s Contact Centre that they undertake a criminal records disclosure through the Disclosure and Barring Service. Following the completion of the volunteer interview the DBS document will be completed and submitted to NACCC for processing by the volunteer Co-Ordinator or a member of the Management Committee. Until the disclosure is returned as defined volunteers will only be allowed to attend MKCCC with permission of the Co-Ordinator and even then only under supervision and guidance
2. All volunteers must have a DBS disclosure undertaken every three years.
3. NACCC is a registered umbrella body processing DBS disclosures for its Member Centres.

Recruitment

4. All advertisements for positions within MKCCC including as volunteers will make clear that a Disclosure and Barring Service disclosure will be requested in the event of a successful application
5. In accordance with MKCCC’s policy on rehabilitation of offenders policy it will also make clear that “a criminal record will not necessarily be a bar to obtaining a position”. See separate policy for details.
6. Consent will be obtained for the DBS disclosure to be undertaken (by way of the signed application form).
7. Milton Keynes Children’s contact centre will review any information listed in a Disclosure and in accordance with the DBS Code of Conduct in accordance with their policy on Rehabilitation of Offenders.

Security & Retention of disclosure information

8. Milton Keynes Children’s Contact Centre takes confidentiality seriously and ensures that all information relating to disclosures are kept in a secure place. See separate policy.
9. Only relevant volunteers and members of Management Committee have access to this.
10. DBS returns one copy of each disclosure per application to the applicant named in the disclosure.
11. Disclosures must be shown to the Contact Centre Co-ordinator who is responsible for this aspect. They will update the Centre’s records and address any issues with the relevant personnel.

Levels of disclosure

12. Milton Keynes Children’s Contact Centre processes all disclosures at the level of “enhanced” as defined by DBS.
13. DBS do not currently charge for disclosures on volunteers and whilst this continues NACCC will continue to process volunteer application without charge.
14. There is a charge for any paid contractors or employees and this cost will be met by Milton

Keynes Children's Contact Centre unless NACCC have the funds to do so and have agreed to meet said cost

W Privacy Policy

Our Privacy Policy explains:

What information we collect and how we collect it
Why and how we use your information.
How long we keep your information
How we may share your information
Your rights on the information we hold about you
Security-how we keep your information safe
Changes to this Privacy Policy
How to contact us

The Data Controller is Milton Keynes's Children's Contact Centre

Information We Collect

In order to provide our services and for the other purposes set out in Use of Information below, we collect and process Personal Data from the users of our Contact Centre. We may collect the following information

- Personal information (for example, your name, email address, mailing address, phone numbers, date of birth and address)
- Sensitive Personal Data
- Attendance information (such a attended, number of absences and absence reasons)
- Safeguarding incidents

From time to time and as permitted by applicable law(s), we may collect Personal Data about you and update any existing Personal Data that we currently hold from other third-party sources

We collect your information from

- Self Referral Forms
- Referrals from organisations e.g. Cafcass, Family Solicitors
- Pre visit checklist

We may also collect information from telephone conversations, emails and written and verbal communications and from records of the Contact Centre sessions.

How we Use of Information

Your Personal Data may be used in the following ways:

- To provide our services to you,
- To respond to your requests and inquiries,
- To improve our services, for example questionnaires
- To request your participation in surveys, or other initiatives which help us to gather information used to develop and enhance our services,
- To comply with applicable law(s) (for example, to comply with a search warrant or court order) or to carry out professional ethics/conduct investigations,
- To enable us to provide, to maintain our own accounts and records and to support and manage our employees.

Consent and lawful Processing of data.

Our legitimate interests, which include processing such Personal Data for the purposes of

- providing and enhancing the provision of our services.
- administration and programme delivery
- for dealing with medical needs-any information you provide we must have had explicit consent to use.
- all other cases: that it is necessary for our legitimate interests which are to run the contact centre

How long will we keep your information?

File Type	Retention Period
HR files Employment references Redundancy details	6 years after employment/volunteering ceases
Parental leave	5 years from birth/adoption or 18 if child receives a disability allowance
Disclosure and Barring Service Certificate (formerly Criminal Records Bureau disclosures certificates) obtained as part of the vetting process.	The actual disclosure form must be destroyed after 6 months. However it is advisable that organisations keep a record of the date of the check, the reference number, the decision about vetting and the outcome.
Finance records Income tax, NI returns, income tax records and correspondence with IR, Parental leave, Wages and salary records	HMRC advise you must keep records for 6 years from the end of the last company financial year they relate to, or longer if: they show a transaction that covers more than one of the company's accounting periods.
Supported contact only – Referrals, with court orders or CAFCASS involvement, pre- visit forms, attendance records	Securely disposed of after three years unless a safeguarding or child protection issue
Supported contact only - Self-referrals with NO court order or CAFCASS involvement, pre- visit forms, attendance records	Securely disposed of after one year unless a safeguarding or child protection issue
Information relating to paid/unpaid staff not covered above that are not used for three years should be treated as confidential waste and disposed of as such.	Securely disposed of after three years.
Accident books and paperwork relating to safeguarding or child protection issues about a specific child	Should be kept indefinitely as children can request this information up to the age of 25 years by Local Authorities.

Sharing and Disclosure to Third Parties

We may disclose your Personal Data to third parties from time-to-time under the following circumstances:

- You request or authorise the disclosure of your personal details to a third party.
- The information is disclosed as permitted by applicable law(s) and/or in order to comply with applicable law(s) (for example, to comply with a search warrant or court order).
- The information is provided to service providers who perform functions on our behalf.

- Hosting providers for the secure storage and transmission of your data
- Legal and compliance consultants, such as external counsel, external auditors
- Technology providers who assist in the development and management of our web properties

Subject Access/User Rights

As a user, you are subject to the following rights:

- The right to be informed of the use of your Personal Data
- The right to access and/or to require the correction or erasure of your Personal Data
- The right to block and/or object to the processing of your Personal Data
- The right to not be subject to any decision based solely on automated processing of your Personal Data
- In limited circumstances, you may have the right to receive Personal Data in a format which may be transmitted to another entity.

If you have a complaint in relation to the processing of your data carried out under this Privacy Policy, you have the right to lodge a complaint with the Information Commissioner Office .

You may seek to exercise any of these rights by updating your information online (where possible) or by sending a written request to

Milton Keynes Childrens Contact Centre
PO BOX 1549
Bedford
MK43 6AX

Information security

We are working to protect your personal information that we hold, its confidentiality, integrity and availability.

- We review our information collection, storage and processing practices, including physical security measures, to guard against unauthorized access to systems.
- We restrict access to personal information to contact centre staff and volunteers subject to strict confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.
- We have Security Information Policy in place which defines the measures we take to protect your personal information. We use a combination of technology and procedures to ensure that our paper and computer systems are protected, monitored and are recoverable.
- We only use third party service providers where we are satisfied that they provide adequate security for your personal data.

Compliance and cooperation with regulatory authorities

We regularly review our compliance with our Privacy Policy. If we receive formal written complaints, we will contact the person who made the complaint to follow up. We work with the ICO to resolve any complaints regarding the transfer of personal data that we cannot resolve with our users directly.

Changes

Our Privacy Policy may change from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent.

X Security Incident Response Procedure

Introduction

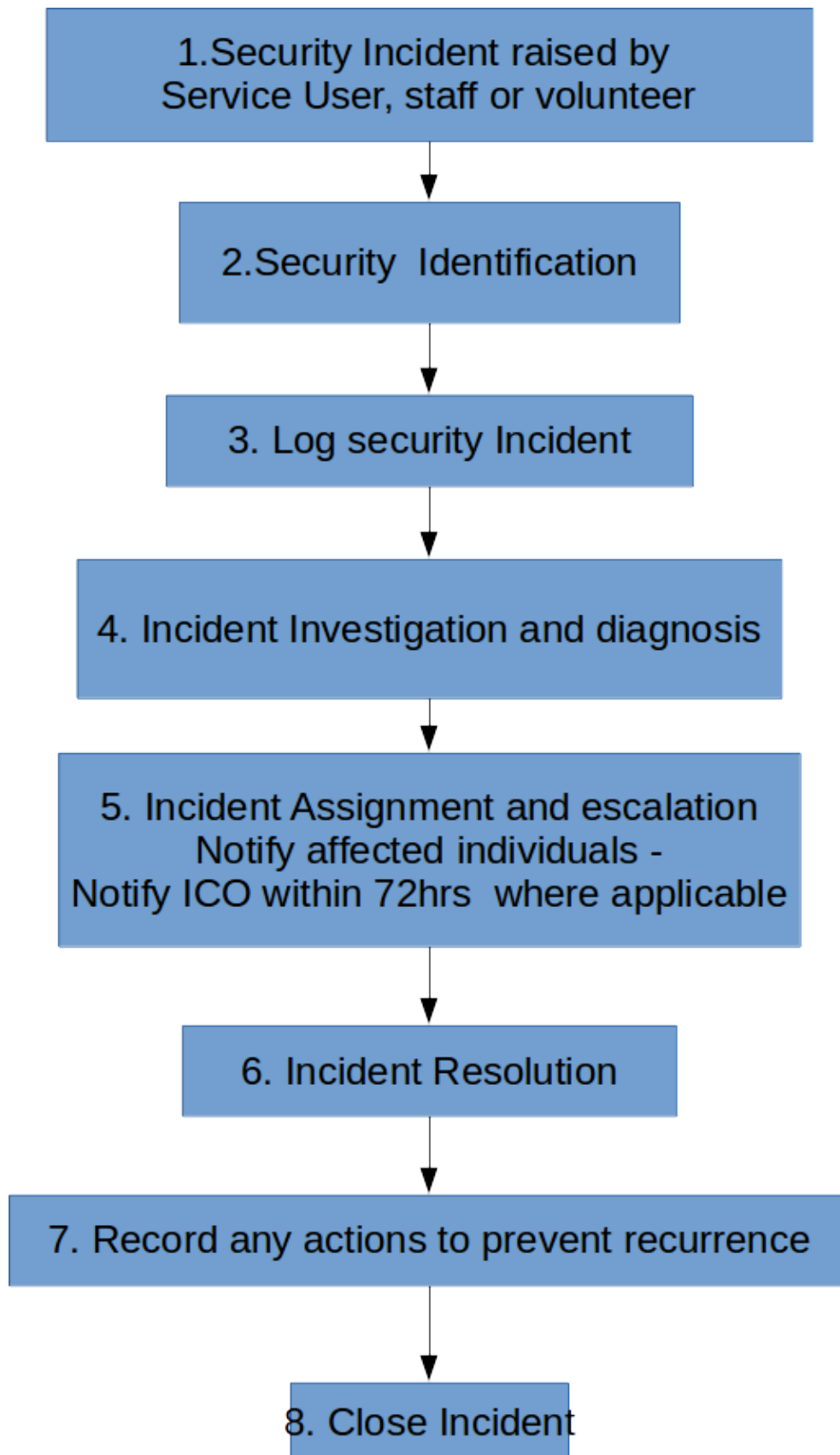
Milton Keynes Childrens Contact Centre will manage any security incidents. This procedure details the actions and roles required when a security incident occurs. It is provided as guidance to staff. All security incidents are recorded. A security incident are issues that potentially impact on the confidentiality, integrity or availability of the centres systems or services.

Procedure

Security incidents will be reported to the Co-Ordinator in the first instance (or deputy in the event of their absence).

On receipt of the security incident report the Co-Ordinator will take the following actions:

1. Receive notification that an incident has occurred from a volunteer or service user e.g. stolen laptop, or complaint
2. Confirm the type of incident and gather any additional [information required by the ICO](#)
3. Log the incident including a brief description, time and date of the incident, who notified the incident and assign a [priority](#) High, Medium or Low
4. Notify a trustee
5. Investigate the incident
6. Diagnose the incident and identify any actions required to resolve the incident see [Incident Types and Responses](#). Where necessary escalate to ICO as soon as possible and within 72hrs. Notify any affected individuals.
7. Incident Resolved -update incident record with details of actions taken and results of any investigation regarding the cause whether this was human error or a systemic issue
8. Record any details of how recurrence can be prevented – whether this is through better processes, further training or other corrective steps.
9. Close incident



Responses

The standard responses are:

Personal Data leakage Response

If the incident results in the loss of personal data as defined in the DPS (2018) / GDPR then it must be reported to the ICO. :

Examples of a data breach Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

Under the GDPR there is a requirement for organisations to report a personal data breach that affects people's rights and freedoms, without undue delay and, where feasible, not later than 72 hours after having become aware of it. Organisations should be aware that the ICO will have the ability to issue fines for failing to notify and failing to notify in time. Fines can be avoided if organisations are open and honest and report without undue delay, which works alongside the basic transparency principles of the GDPR.

Serious breaches should be reported to the ICO using our DPA security breach helpline on 0303 123 1113 (open Monday to Friday, 9am to 5pm). Select option 3 to speak to staff who will record the breach and give you advice about what to do next.

Further information can be found at;
https://ico.org.uk/media/for-organisations/documents/1536/breach_reporting.pdf

Criminal Attack Response

If the incident is a potential attack incident, the incident will be reviewed and if an attack is confirmed it should be reported as such to the customer who will report it to the relevant law enforcement body. The Milton Keynes Childrens Contact Centre will zip and sign the relevant evidence, collected from logs etc. earlier. This evidence will be made available to the customer as required, subject to confidentiality undertakings (it will contain non-customer specific sensitive information). The complete pack will be preserved for subsequent law enforcement action.

Denial of Service(DoS) Response

This has become an increasing threat recently, often manifested as a distributed denial of service (DDoS) attack, which is more difficult to combat. Access to bot-nets is becoming increasingly widespread so that individuals with grievances have access to facilities hitherto only available to criminal organisations. The attack could be directed at Milton Milton Keynes Childrens Contact Centre or Milton Keynes Childrens Contact Centre could be subject to collateral damage due to attacks on adjacent services. DoS and particularly DDoS attacks can result in:

- The Milton Keynes Childrens Contact Centre web site being unable to respond to legitimate transactions as they are swamped by a flood attack. This would be a direct attack from a low capacity resource.
- The hosting site being forced to suspend the service to enable other services on their site to continue. If this is a direct attack, Milton Keynes Childrens Contact Centre would be suspended, if Milton Keynes Childrens Contact Centre was suffering collateral damage this would re-open Milton Keynes Childrens Contact Centre.
- The ISP switching off access to the Milton Keynes Childrens Contact Centre in order to prevent their service from being overwhelmed. Again, if this is a direct attack, Milton Keynes Childrens Contact Centre would be suspended, if Milton Keynes Childrens Contact Centre was suffering collateral damage

this would re-open Milton Keynes Childrens Contact Centre

For a DoS attack or low capacity¹ DDoS, action from the hosting provider to block traffic from specific incoming IP addresses should be taken. Arrangements for this action will be made with each hosting site.

For DDoS, the customer should be contacted and, subject to their agreement Emergency DDoS protection should be put in place. As this is chargeable, the customer's agreement and order must be obtained before invoking the service.

The Milton Keynes Childrens Contact Centre will maintain a list of suitable service providers, contact details and costs.

Malware Discovery

Where malware is discovered by routine application of anti-malware measures, this should be logged.

Web Exploit

In most cases, this will be a new exploit. We need to cover, routinely, the OWASP exploits (see <http://www.ibm.com/developerworks/library/se-owasptop10/index.html>) , although some variants may need modified responses. On discovery of a web exploit we will put devise and put into place an emergency fix / procedure to block the exploit. We will check against the OWASP list if the exploit is know. If it is not, we will inform OWASP of the exploit, providing details as required. If it is a deliberate act, we will invoke our Criminal Attack Response, including the session logs in our evidence pack.

Definitions

Incidents will be classified according to their impact on the Milton Keynes Childrens Contact Centre systems or services.

Level	Impact
High	Actual breach effecting the availability, integrity or confidentiality of the Milton Keynes Childrens Contact Centre critical information assets.
Medium	Vulnerability discovered which, if exploited could give rise to a data breach
Low	Other types of security incident

1

Where the number of attacking IP addresses are such that all the attacking addresses could be filtered.

ICO data required

A description of the nature of the personal data breach including, where possible:

- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Y Privacy Impact Assessment

- **Introduction**

In order to demonstrate compliance with the DPA and subsequently the GDPR, as well as having the required evidence for compliance with the pathway statements made to OGSIRO, a Privacy Impact Assessment is required.

- **Method**

To demonstrate compliance with GDPR and DPA, a PIA is defined here in line with the ICO template.

- **Compliance with DPA Principles**

- **Principle 1**

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

The use of personal data in Child Contact Centre is permitted As defined in the NACCC-gdpr-documentation-controller spreadsheet.

The use of sensitive personal data in Child Contact Centre is permitted under DPA 2018 as defined in the NACCC-gdpr-documentation-controller spreadsheet.

- **Principle 2**

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

The data is obtained to carry out the legitimate interests of the contact centre and is limited to that.

- **Principle 3**

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Data is collected as required by the business need.

- **Principle 4**

Personal data shall be accurate and, where necessary, kept up to date.

Data is collected as a record of communications and its provenance is known.

- **Principle 5**

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

Data is retained for the period defined in the data retention policy. The retention periods are derived from:

- 1) to comply with legal requirements
- 2) to comply with contractual requirements specified by the referrer, these period are governed by the referrers legal responsibilities and data policies.
- 3) for operational purposes, e.g., maintain evidence of attendance to provide details to court, local authorities and parents.

○ Principle 6

Personal data shall be processed in accordance with the rights of data subjects under this Act.

Yes.

○ Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

Compliant, the systems have been designed to ensure only those identified, authorised and authenticated have access. All data is encrypted at rest and in transit.

○ Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

All data is retained within the UK, in the EEA or under Privacy Shield arrangements.

● Information Flows

Data is gathered from Referrers or Data Subjects and can subsequently be updated by Data Subjects. Generally, personal data is not transferred to any third party with the exception of:

1. The certificated data processor – we rely on their ISO 27001 and SOC 1/2 assertions together with detailed technical assurance on encryption.
2. Limited employee data can be passed, with their permission to those requiring references from us.
3. Limit data on attendances can be passed to legitimate authorities.
4. Under some circumstances data can be pass on formal request to the Family Courts

Z Information Security Policy

Introduction

This information security policy is a key component of the Child Contact Centre (CCC) management framework. It sets the requirements and responsibilities for maintaining the security of information within CCC. This policy may be supported by other policies and by guidance documents to assist putting the policy into practice day-to-day.

○ Purpose

○ This policy is intended to support CCC business objectives and, without undue restrictions, protect its volunteers, employees, clients, contractors, third parties and the business from illegal or damaging events or actions by individuals, either knowingly or unknowingly.

The objective of this policy is to define the CCC's policies that in order to protect the confidentiality, integrity and availability of CCC's information assets, its reputation and the safety of all its stakeholders. Everyone who works in or with the Company has a duty and a responsibility to comply with these policies.

○ Applicability

○ The policy applies to the use of all CCC IT equipment and information systems belonging to or managed by the company, including but not limited to: laptops, workstations, servers, networks, supporting infrastructure, telephones, telephony systems, mobile devices (such as smart-phones), removable media, third-party systems and any cloud-based infrastructure, platforms or services.

This policy is applicable to all CCC employees both permanent and temporary, volunteers, contractors, agency workers and any third parties who provide services. It is the responsibility of all such individuals to read and understand this policy, and to conduct activities in full accordance with it. If there is any uncertainty, employees should consult the centre coordinator.

○ Aim and Scope of this policy

○ The aims of this policy are to set out the rules governing the secure management of our CCC information by:

- preserving the **confidentiality, integrity and availability** of our business information
- ensuring that all members of staff are aware of and fully comply with the relevant **legislation** as described in this and other policies

- ensuring an approach to security in which all members of staff fully understand their own **responsibilities**
- creating and maintaining within the organisation a level of **awareness** of the need for information
- detailing how to **protect** the information assets under our control

This policy applies to all information/data, information systems, networks, applications, locations and staff of CCC or supplied under contract to it.

○ **Responsibilities**

Ultimate responsibility for information security rests with the Trustees but the centre coordinator or Administrator shall be responsible for managing and implementing the policy and related procedures.

Responsibility for maintaining this Policy, the business Information Risk Register and for recommending appropriate risk management measures is held by the Centre coordinator. Both the Policy and the Risk Register shall be reviewed by the Trustees at least annually.

Coordinators are responsible for ensuring that their permanent staff, volunteers temporary staff and contracts are aware of:-

- The information security policies applicable in their work areas
- Their personal responsibilities for information security
- How to access advice on information security matters

All staff and volunteers shall comply with the information security policy and must understand their responsibilities to protect the Centre's data. Failure to do so may result in disciplinary action.

Coordinators shall be individually responsible for the security of information within their business area.

Each member of staff shall be responsible for the operational security of the information systems they use.

Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

Access to the organisation's information systems by external parties shall only be allowed where a contract that requires compliance with this information security policy is in place. Such a contracts shall require that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

In order to ensure compliance, the following is needed:

- Appoint a Trustee with specific responsibilities for security – the risk owner;

- Appoint a person responsible for with day-to-day security;
- Identify individuals responsible for specific information assets such as: Referral / client information, staff or finance information. They need to be able to understand the threats likely to compromise the information.
- Ensure that all individuals with designated security responsibilities undertake appropriate training for their role.

Risk Assessment and Management

-
- The CCC will adopt a risk assessment methodology as part of a holistic risk management approach covering all areas of protective security across its organisation. It will include a risk register (with assigned risk owners) recording any specific vulnerabilities or security risks, the control measures taken to mitigate these risks, and any adjustments over time following changes to the threat environment. Subject to security considerations, the risk register should be made widely available within the organisation to ensure all business units have an input It will include:
 - A statement of the IT assets deployed by the CCC – the asset register.
 - A statement of the threats faced by the CCC
 - A statement of the impacts of compromise of the information assets
 - A statement of the tolerable level of risk (the risk appetite)
 - Record the application of proportionate selection of technical, procedural, personnel and physical security controls to manage the identified risks to a level that the business can tolerate;
-

For all projects that include the use of personal information the CCC must assess the privacy risks to individuals in the collection, use and disclosure of the information and a Privacy Impact Assessment (PIA) / Data Protection Impact Statement (DPIA), as recommended by the Information Commissioner, must be carried out as a minimum

- Have the ability to regularly audit information assets and ICT systems to check compliance and extract data in the event of an incident;
-
- Where shared systems or services are used, the CCC must satisfy themselves that the use of these systems or services can be managed within its own risk appetite.

○ Legislation

1. CCC is established as a not for profit charity
2. CCC is required to abide by certain UK, European Union and international legislation.
3. In particular, CCC is required to comply with:
 - The Data Protection Act (2018)(Including GDPR)

- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
 - The Copyright, Designs and Patents Act (1988)
 - The Computer Misuse Act (1990)
 - The Health and Safety at Work Act (1974)
 - Human Rights Act (1998)
 - Freedom of Information Act 2000
- **Personnel Security**
- Volunteer Agreement
 - Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a security and confidentiality clause.
 - References for new staff shall be verified and a passport, driving license or other document shall be provided to confirm identity.
 - Information security expectations of staff shall be included within appropriate job definitions.
 - Whenever a staff member leaves the company their accounts will be disabled the same day they leave.

Information Security Awareness and Training

- The aim of the training and awareness programmes are to ensure that the risks presented to information by staff errors and by bad practice are reduced.
- Information security awareness training shall be included in the staff induction process and shall be carried out annually for all staff
- An on-going awareness programme shall be established and maintained in order to ensure that staff awareness of information security is maintained and updated as necessary.

Intellectual Property Rights

- The organisation shall ensure that all software is properly licensed and approved by the Coordinator / administrator. Individual and CCC intellectual property rights shall be protected at all times.
- Users breaching this requirement may be subject to disciplinary action.

Access management

Physical Access

- Only authorised people who have a valid and approved business need shall be given access to areas containing information systems or stored data.

Identity and passwords

- Passwords must offer an adequate level of security to protect systems and data
- All passwords shall be eight characters or longer and contain at least two of the following: upper case letters, lower-case letters and numbers
- All administrator-level passwords shall follow NCSC guidelines (see <https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach>)
- Where available, two-factor authentication shall be used to provide additional security

User Access

- Access to information shall be based on the principle of “least privilege” and restricted to authorised users who have a need to access the information.

Administrator-level access

- Administrator-level access shall only be provided to individuals with a business need who have been authorised by the CCC Coordinator.
- A list of individuals with administrator-level access shall be held by the CCC Coordinator and shall be reviewed every 6 months
- Administrator-level accounts shall not be used for day-to-day activity. Such accounts shall only be used for specific tasks requiring administrator privileges.

Application Access

- Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators.
- Authorisation to use an application shall depend on a current licence from the supplier.

Hardware Access

- Where indicated by a risk assessment, access to the network shall be restricted to authorised devices only

System Perimeter access (firewalls)

- The boundary between business systems and the Internet shall be protected by firewalls, which shall be configured to meet the threat and continuously monitored.
- All servers, computers, laptops, mobile phones and tablets shall have a firewall enabled, if such a firewall is available and accessible to the device's operating system.
- The default password on all firewalls shall be changed to a new password that complies to the password requirements in this policy, and shall be changed regularly
- All firewalls shall be configured to block all incoming connections.
- If a port is required to be opened for a valid business reason, the change shall be authorised following the system change control process. The port shall be closed when there is no longer a business reason for it to remain open.

Monitoring System Access and Use

- An audit trail of system access and data use by staff shall be maintained wherever practical and reviewed on a regular basis.
- The CCC reserves the right to monitor and systems or communications activity where it suspects that there has been a breach of policy in accordance with the Regulation of Investigatory Powers Act (2000).

- **Asset Management**

Asset Ownership

- Each information asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

Asset Records and Management

- An accurate record of CCC information assets, including source, ownership, modification and disposal shall be maintained.
- All data shall be securely wiped from all hardware before disposal.

Asset Handling

- CCC shall identify particularly valuable or sensitive information assets through the use of data classification.

- All staff are responsible for handling information assets in accordance with this security policy. Where possible the data classification shall be marked upon the asset itself.
- All company information shall be categorised according to the risk assessment and shall be handled according to the risk appetite defined in that policy.

Removable media

- Only CCC approved removable media (such as USB memory sticks) shall be used to store CCC data it will be encrypted and its use shall be recorded.
- Removable media of all types that contain software or data from external sources, or that has been used on external equipment, require the approval of the -CCC Coordinator before they may be used on business systems. Such media must be scanned by anti-virus before being used.
- Where indicated by the risk assessment, systems shall be prevented from using removable media.

Users breaching these requirements may be subject to disciplinary action.

Mobile working

- Where necessary, staff may use supplied mobile devices such as phones, tablets and laptops to meet their job role requirements
- Use of personal mobile devices for business purposes (whether business-owned or personal devices) requires the approval of the CCC Coordinator.
- Such devices must have anti-malware software installed (if available for the device), must have PIN, password or other authentication configured, must be encrypted (if available for the device) and be capable of being remotely wiped. They must also comply with the software management requirements within this policy.
- Users must inform the CCC Coordinator immediately if the device is lost or stolen and business information must then be remotely wiped from the device.

Personal devices / Bring Your Own Device (BYOD)

- Where necessary, staff may use personal End User Devices (EUDs), i.e., mobile phones, laptops, tablets etc., to access email. Content may only be stored on encrypted devices approved by the Coordinator. The device must be recorded in the asset register and must be configured to comply with the **mobile working section** and other relevant sections of this policy.
- No other personal devices are to be used to access business information

Social Media

- Social media may only be used for business purposes by using official business social media accounts with authorisation. Users of business social media accounts shall be appropriately trained and be aware of the risks of sharing sensitive information via social media.
 - Access to all CCC business facilities and functions will be restricted to duly identified and authenticated authorised individuals.
 - Social media accounts used by the Child Contact Centre shall be protected by strong passwords in-line with the password requirements for administrator accounts.
 - Users shall behave responsibly while using any social media whether for business or personal use, bearing in mind that they directly or indirectly represent centre. If in doubt, consult the CCC Coordinator.
 - Users breaching this requirement may be subject to disciplinary action.
- **Physical and Environmental Management**
 - In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards. Physical security accreditation should be applied if necessary.
 - Systems shall be protected from power loss by UPS if indicated by the risk assessment.
 - Systems requiring particular environmental operating conditions shall be maintained within optimum requirements.

- **Computer and Network Management**

Operations Management

- Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the CCC Coordinator .

System Change Control

- Changes to information systems, applications or networks shall be reviewed and approved by the CCC Coordinator .

Accreditation

- The CCC shall ensure that all new and modified information systems, applications and networks include security provisions.

- They must be correctly sized, identify the security requirements, be compatible with existing systems according to an established systems architecture (as required) and be approved.

Software Management

- All application software, operating systems and firmware shall be updated on a regular basis to reduce the risk presented by security vulnerabilities.
- All software security updates/patches shall be installed within 7 days of their release.
- Only software which has a valid business reason for its use shall be installed on devices used for business purposes
- Users shall not install software or other active code on the devices containing business information without permission from [title].
- For the avoidance of doubt, all unnecessary and unused application software shall be removed from any devices used for business purposes.

Local Data Storage

- Data stored on the business premises shall be backed up regularly and restores tested at appropriate intervals (at least monthly).
- A backup copy shall be held in a different physical location to the business premises
- Backup copies of data shall be protected and comply with the requirements of this security policy and be afforded the same level of protection as live data.

Data Protection

- Data in transit will always be protected by encryption (TLS or IPsec)
- Data at rest will be protected as follows:
 - Personal data will be encrypted, (this is in line with GDPR requirements) and keys held by trusted custodians.
 - Other sensitive information, i.e., information where the confidentiality impact is assessed at medium or above, will be encrypted and keys held by trusted custodians.
 - All other data will be protected by restricting access to identified and authenticated authorised individuals.

External Cloud Services

- Where data storage, applications or other services are provided by another business (e.g. a 'cloud provider') there must be independently audited, written

confirmation that the provider uses data confidentiality, integrity and availability procedures which are the same as, or more comprehensive than those set out in this policy.

Protection from Malicious Software

- The business shall use software countermeasures, including anti-malware, and management procedures to protect itself against the threat of malicious software.
- All computers, servers, laptops, mobile phones and tablets shall have anti-malware software installed, where such anti-malware is available for the device's operating system
- All anti-malware software shall be set to:
 - scan files on-access
 - automatically check for, daily, virus definitions and updates to the software itself and install new versions when they become available
 - block access to malicious websites

Vulnerability scanning

- The business shall have a regular vulnerability scan of all external IP addresses carried out by a suitable external company
- The business shall act on the recommendations of the external company following the vulnerability scan in order to reduce the security risk presented by any significant vulnerabilities
- The results of the scan and any changes made shall be reflected in the company risk assessment and security policy as appropriate.

Information security incidents

- All breaches of this policy and all other information security incidents shall be reported to the Centre Coordinator.
- All other information security incidents shall follow a SIR (Security Incident Response) procedures which require:
 - If required as a result of an incident, data will be isolated to facilitate forensic examination.
 - Information security incidents shall be recorded in the Security Incident Log
 - The risk assessment and this policy shall be updated if required to reduce the risk of a similar incident re-occurring.

- Identify and assign information security roles and responsibilities appropriate to the size, structure and business function of their organisation;
- Adopt policies, procedures and controls to ensure information assets are identified, valued, handled, stored, processed, transmitted, shared and destroyed in accordance with legal requirements;
- Manage the risks associated with digital continuity and records management in respect of all data held electronically, particularly in the event of upgrades in technology, transferral of data into archives and the overall life cycle of data;
- Assess any security and business risks before deciding to outsource or offshore information and/or services. Data or services that relate to or directly support national security should not normally be off shored.

Privacy Statements

The Contact Centre must provide a privacy statement to all data subjects, for which we hold data. This should be in line with ICO guidance about following GDPR.

Procedures must be in place covering the receipt, storage, correction and deletion of personal, including special category, data.

Valuing and Classification Assets

The Contact Centre must ensure that information assets are valued, handled, shared and protected in line with the standards and procedures set out in legal obligations and undertakings

To comply with this requirement CCC will ensure that:

- Information and other assets are valued according to the definitions the classification policy and are clearly and conspicuously marked. Where this is impractical (e.g. a building or physical asset) staff must be made aware of the protective controls required;
- Assets are protected in line with the risk appetite and countermeasures, defined in the risk assessment, throughout their life-cycle from creation to destruction to ensure a proportionate level of protection against the real and/or anticipated threats faced by such assets;
- Access to sensitive assets is only granted on the basis of a genuine need to know and an appropriate level of personnel security control;
- Where information is shared for business purposes the CCC must ensure the receiving party understands the obligations and protects the assets appropriately;

Risk Assessment and Accreditation of ICT Systems

1. Business Continuity and Disaster Recovery Plans

- The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.
- The following arrangement shall be followed:

Risk	Likelihood Score	Mitigation Plan
Loss of staff: As a contact centre many skill sets are very critical to the organisation.	B. High Impact, Low Likelihood.	Capture as much information as possible. Prioritise having staff and volunteers that provide redundancy.
Loss of premises: e.g. building burns down.	B. High Impact. Low Likelihood.	
Loss of key supplier:	D. Low Impact. Low Likelihood.	Contractual arrangement shall be put into place which supports the transfer of services to alternative suppliers if required.

Reporting

- The Coordinator shall keep the trustees informed of the information security status of the organisation by means of regular reporting.

AA Personal Commitment Statement for Volunteers

Personal Commitment Statement for Staff & Volunteers to the Security of Data and Systems

The Milton Keynes Childrens Contact Centre contain personal and special category data, as defined by the Data Protection Acts 2018 / GDPR.

Breaches - Breaching the security of this information carries significant penalties and well as breaching the trust placed in us by our clients. Controls and measures have been put in place to control access to and export of this information, but chiefly relies on the care taken by staff in the use of computer systems and any other handling of information.

To qualify for access to the Milton Keynes Childrens Contact Centre computer systems it is a requirement that all users with a right to access our systems must read and agree to follow these requirements particularly those which relate to the use the secure custodianship and controlled release of information. Please read the following and confirm that you have read and understood what is required of you by completing and signing the section at the end of this document. By completing the action, you are confirming that you will follow the rules.

All Milton Keynes Childrens Contact Centre system users

- are responsible for their unique user login details including User name or ID and password. (user ID and password, or other mechanism as provided) and e-mail address;
- will not use a colleague's credentials to access the systems and will equally ensure that my credentials are not shared and are protected against misuse;
- will protect such credentials to the same extent as the information they may be used to access,
- will not attempt to access any computer system that I have not been given explicit permission to access;
- will not use, store or send information they know or suspect to be unacceptable within the context and purpose for which it is being used.
- will protect any material, whatever the sensitivity sent, received, stored or processed on the system ;
- will not send sensitive information over public networks such as the Internet unless approved encryption has been applied to it;
- will always check that the recipients of e-mail and any other types messages are correct so that potentially sensitive or protectively marked information is not accidentally released into the public domain;
- will disclose information received via the system only on a 'need to know' basis;
- will seek to prevent inadvertent disclosure of sensitive information by avoiding being overlooked when working, by taking care when printing information and by carefully checking the distribution list for any material to be transmitted;
- will securely store or destroy any printed material;
- will not leave my computer unattended in such a state as to risk unauthorised disclosure of information
- will inform immediately if they detect, suspect or witness an incident that may be a breach of security;
- will not attempt to bypass or subvert system security controls or to use them for any purpose other than that intended;

- will not remove information the Milton Keynes Childrens Contact Centre systems without appropriate approval, specifically it should not be transferred to person computer devices;
- will take precautions to protect all computer media and portable computers when carrying them outside our premises (e.g. leaving a laptop unattended or on display in a car such that it would encourage an opportunist thief);
- will not introduce viruses, Trojans or other malware into the system ;
- will comply with the Data Protection Act 2018 and any other legal, statutory or contractual obligations
- will accept and understand that their use of Milton Keynes Childrens Contact Centre systems may be monitored and/or recorded for lawful purposes.
- if I have reason to suspect that another person has unauthorised access to my email account or any systems they should not have access , I will notify the Milton Keynes Chlidrens Contact Centre Coordinator at the first available opportunity.
- I will comply with the Data Protection Act, Computer Misuse Act and all other IT related legislation that my employer informs me are relevant.
- Have read, understand and accept Milton Keynes Childrens Contact Centre privacy and information security policy.

I have read, understand and agree to comply with the above.

Signed	
Date	
Name	
Organisation	