

Safeguarding and Welfare Requirement: Child Protection

Providers must have and implement a policy, and procedures, to safeguard children.



1.7 ICT Misuse policy

Policy statement

- *The ICT (Information and Communication Technology) Misuse Policy aims to ensure any allegation, which is to be made in respect of the intentional or unintentional misuse of any online technologies, is to be addressed to in a responsible and calm manner. This is to include any known or suspected breaches of the Acceptable Use Policy and the Online Safety Policy.*
- *Allegations are to be dealt with promptly, sensitively and fairly in line with agreed procedures. The ICT Misuse Policy will also outline the sanctions that are to be applied should an incident occur.*
- *The overall priority will be to ensure the safety and wellbeing of children at all times. Should it be suspected at any stage that a child or young person may have been or is considered to be subject to abuse, the Safeguarding Policy and Procedures must be implemented with immediate effect. These procedures are also to be followed should an allegation of abuse be made against any employee, Leader, volunteer or student. The Safeguarding Children and Child Protection Policy (1.2) is to take precedence over all others, and referrals must be made to the appropriate agency as deemed necessary.*

Procedures

In the event of alleged misuse by a child or young person

- Should a child be found to inappropriately misuse ICT the following sanctions will be applied:
 - **Step 1:** Should it be considered that a child or young person has deliberately misused ICT by not adhering to the Acceptable Use Agreement, a letter will be sent to the parent or carer outlining the issue. The child or young person may be temporarily suspended from a particular activity.
 - **Step 2:** If there are to be further incidents of misuse, the child will be suspended from using the internet or other relevant technology for an increased period of time. The parent or carer will be invited to discuss the incident in more detail with the Designated Lead Practitioner (DLP) for safeguarding and the most appropriate course of action will be agreed.
 - **Step 3:** The sanctions for misuse can be escalated at any stage, should it be considered necessary. In the event that misuse is deemed to be of a serious nature, steps 1 and 2 can be omitted. Should a child be considered to be at risk of significant harm, the Safeguarding Policy must also be applied. Allegations of serious misuse will be reported to the most appropriate agency, for example, the Police or Children's Social Care.

In the event of alleged misuse by parents/carers

- Should it be alleged, that a parent or carer is to have misused any ICT resource in an abusive, inappropriate or illegal manner, a report is to be made to Centre Manager and DLP immediately. The Centre Manager will inform the Chair of the Committee and will investigate as far as possible/appropriate. If the allegation of misuse concerns the Tapestry system then access to this may be restricted or denied. Should allegations relate to abuse or unlawful activity, Children's Social Care, the Local Authority Designated Officer, Ofsted and/or the Police will be notified as applicable.

In the event of alleged misuse by a member of staff

- All incidents are to be dealt with on an individual case by case basis, and an escalating tariff of agreed sanctions are to be put in place.
- The context, intention and impact of each incident are to determine the response and actions to be taken. This will allow for a degree of flexibility as to how sanctions are to be applied, subject to the need for other policies to be implemented. For example, a series of minor incidents by one individual is likely to be treated differently than should it be deemed a one-off occurrence; similarly unintentional and intentional access to inappropriate websites are to instigate different levels of intervention and sanctions.
- All online safety incidents are to be recorded and monitored, and any potential patterns in behaviours should be identified, to enable such issues to be addressed proactively and for protection to be afforded.
- Misuse is to be categorised under the three headings of 'minor incidents', 'significant incidents' and 'serious incidents'.

Minor incidents

- The following procedure is to be followed should an incident be considered minor.
 - The incident is to be reported to the Centre Manager and DLP. A written incident record to be made and the situation is to be monitored.
 - The context, intention and impact of such misuse must also be considered. Where deemed necessary the incident is to be escalated to a 'significant' or 'serious' level.

Significant incidents

- There will always be the possibility that through access to the internet children and young people may gain unintentional access to inappropriate materials. Such material may not be illegal, but is not to be considered suitable in a childcare environment and/or to be age appropriate.
- An open reporting policy is to be in place which means that all inadvertent breaches and access to inappropriate materials must be reported. The non-reporting of such breaches are to result in the concern being escalated.
- The following procedure is to be followed should an incident be considered significant.
 - The incident is to be reported to the Centre Manager. A written incident record is to be made.

- The context, intention and impact of such misuse must also be considered. Where deemed necessary the incident is to be escalated to a 'serious' level.
- Appropriate action is to be agreed between the Centre Manager and the Chair of the Committee.
- If the incident should relate to the inadvertent access to an inappropriate website, it is to be added to the banned or restricted list and filters are to be applied, where relevant.
- In respect to misuse towards children; parents/carers are to be informed of the alleged incident and are to be advised of any actions to be taken as a result.

Serious incidents

- It must be ensured that all serious incidents will be dealt with promptly and reported to the Centre Manager, DLP and the Chair of the Committee immediately.
- The context, intention and impact of the alleged misuse must be considered.
- Appropriate action is to be agreed between the Centre Manager, DLP and the Chair of the Committee. All details are to be accurately and legibly recorded. The reason why any decision is made will be also be noted.
- Should it be considered at any stage that a child is or has been subject to abuse of any form, the Safeguarding children and Child Protection Policy (1.2) will be implemented with immediate effect. A referral will be made to Children's Social Care and the Police, where applicable.
- Should the incident relate to an allegation made against an employee, Manager, volunteer or student; and there is a suggestion that a child has been subject to any form of abuse, the Safeguarding Children and Child Protection Policy will again be implemented with immediate effect. The Local Authority Designated Officer must be contacted in the first instance in respect of any allegation made against an adult. The Police and Ofsted must also be contacted.
- It is to be ensured that no internal investigation or interviews are to be carried out in respect of any allegations, unless it is to be explicitly requested otherwise by an investigating agency.
- It is to be fully recognised that should allegations of abuse be made, Children's Social Care, the Police and/or the Local Authority Designated Officer will be the investigative bodies. It must therefore be ensured that no action is to be taken which could compromise any such investigations.
- Where applicable, any hardware implicated in any potential investigations of misuse is to be secured, so that evidence can be preserved. This may include mobile phones, laptops, computers and portable media technology.
- Internal disciplinary procedures must not be undertaken until investigations by the relevant agencies are to have been completed. Legal or human resources advice should be sought prior to carrying out any internal investigations and/or instigating high-level disciplinary procedures.
- On completion of both internal and external investigations, or sooner where it is to be deemed appropriate, an online safety review is to be undertaken and policies and procedures are to be amended and updated as necessary. A consultation on any proposed revisions will be held with all ICT users as appropriate. Revised policies and procedures will be circulated as applicable.
- By nature, serious incidents will most often involve illegal materials and activities, including the viewing, possession, taking, making and distribution of indecent images; bullying or harassment

through the use of portable media devices, such as mobile phones or grooming. In such situations, these incidents may be instigated by a child, young person or adult.

- The following incidents must always be reported to the Police, Children’s Social Care, Local Authority Designated Officer and Ofsted:

- Discovery of indecent images of children and young people.
- Behaviour considered to be ‘grooming’.
- Sending of obscene materials.

It should be understood, that by not reporting such incidents, an offence may be committed.

- The seriousness of such allegations is to be fully recognised, and it must be ensured that all such incidents are to be reported to the Police immediately. No attempt is to be made to download, print or send any materials found. It should be understood that further offences could be committed by doing so.
- Should potentially illegal material be discovered, as far as is reasonably practical, the equipment or materials found will not be touched. Computers or other devices will not be switched off unless it is authorised to do so by the Police. The focus must be on preventing further access to the illegal content by keeping other individuals out of the immediate area. Where necessary the monitor should be turned off (but the computer should remain on).

Illegal material and activities which must be reported to the Internet Watch Foundation.

- A report is to be made to the Internet Watch Foundation (IWF Internet Watch Foundation <http://www.iwf.org.uk/reporting.htm>) should potentially illegal material, including images of child abuse be discovered. If it is unclear whether the content is to be considered illegal or not, the concern will be reported as a matter of caution.
- Should it be considered that materials are inappropriate but legal, such incidents will generally be dealt with through internal disciplinary procedures. Unless alleged criminal activity and/abuse is suspected, it will not normally be considered necessary to involve the Police or other agencies.

Media attention

- It must be recognised that should a serious incident occur, it will most likely attract intense media interest and speculation. On such occasions, every possible attempt is to be made to ensure that children, parents and carers are protected from such influences.
- An agreed media strategy will be implemented, and statements must only be released by authorised personnel, in accordance with information sharing procedures. In all instances, the prime concern will be the safeguarding and welfare of the children and their families. Advice will be taken from Services for Children and Young People where appropriate before any media engagement is to be undertaken.

This policy was adopted by	_____
On	_____
Date to be reviewed	_____
Signed on behalf of the provider	_____
Name of signatory	_____
Role of signatory (e.g. chair, director or owner)	_____

