

## **Chudleigh Pre-School**

**Registered Charity No: 1028874**

**PLA No: 22478**

### **ICT Misuse Policy**

#### **1 Aim**

The ICT (Information and Communication Technology) Misuse Policy will aim 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 in a responsible and calm manner. This is to include any known or suspected breaches of the Acceptable Use Policy, Camera and Image Policy, Internet Policy and Mobile Technology 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 well-being of children at all times. Should it be suspected at any stage that a child 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, manager, volunteer or student. The Safeguarding Policy is to take precedence over all others, and referrals must be made to the appropriate agency as deemed necessary.

#### **2 Scope**

The ICT Misuse Policy will apply to all individuals who are to have access to and/ or be users of work-related ICT systems. This will include children, parents and carers, pre-school staff, volunteers, students, committee members, visitors, contractors and community users. This list is not to be considered exhaustive.

The policy will be implemented in respect of any potential breaches of the Acceptable Use Policy, Camera and Image Policy, Internet Policy and Mobile Technology Policy.

#### **3 Responsibilities**

The registered person and the Designated Safeguarding Lead (DSL) are to be

responsible for ensuring that the procedures outlined herein will be followed. These procedures are to be considered should an allegation of misuse be made against a child, young person or adult.

#### **4 Policy statement**

Clear and well-publicised policies and procedures which will influence practice, are to be considered the simplest and most effective way for the safe use of ICT to be upheld. Such policies and procedure should ensure the promotion of acceptable use and clearly define those behaviours which are not. The sanctions to be imposed in respect of any incidents of misuse should be identified.

It will be ensured that:

- relevant online safety policies and procedures will be fully implemented, monitored and reviewed. These policies and procedures are to be rigorous, manageable and reflective of practice; and are to be shared with all ICT users. The DSL will be responsible for the management of such policies.
- all ICT users are to be made aware of possible signs of potential misuse. Staff, in particular, will be responsible for observing practice and behaviours, so that any significant changes in such are to be identified at the earliest opportunity.
- all ICT users are to be made aware that the misuse of ICT and/or breaches of relevant policies and procedures are to be taken seriously. All ICT users are to be made aware of the potential sanctions that could be applied should such concerns be raised.
- effective reporting and whistle-blowing procedures are to be in place and promoted.

It is to be acknowledged, however, that no system or procedure can be considered 100 per cent safe, secure and fool-proof. It should therefore be accepted that the potential for ICT to be misused, whether intentionally or unintentionally will remain. The aim of the online safety policies will therefore be to minimise such opportunities and risk.

#### **5 Procedures**

##### **General**

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 pro-actively 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 DSL. A written incident record is 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.

- Sanctions are to be applied in accordance with the Acceptable Use Policy.

#### ***- Significant incidents***

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 DSL. 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 DSL and the registered person.
- 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.

- Sanctions are to be applied in accordance with the Acceptable Use Policy.
- In respect to misuse by children and young people, parents and 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 DSL and the registered person immediately.

The context, intention and impact of the alleged misuse must be considered.

Appropriate action is to be agreed between the DSL and the registered person. 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 or young person is or has been subject to abuse of any form, the Safeguarding Policy 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 or young person has been subject to any form of abuse, the Safeguarding 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, tablets, laptops, computers and other 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 tablets - 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.

- Incidents of promotion of terrorism or extremism, as well as criminally racist material or other criminal conduct, should be reported to the Police.

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 remain on).

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

A report is to be made to the Internet Watch Foundation<sup>1</sup> 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.

<sup>1</sup> IWF Internet Watch Foundation <http://www.iwf.org.uk/reporting.htm>

## **7 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, young people and their families. Advice will be taken from Children and Young Peoples' Services where appropriate before any media engagement is to be undertaken.

Chudleigh Pre-school: ICT Misuse Policy

Adopted at Committee Meeting

10 July 2012

Reviewed September 2014, October 2017, September 2021

**Related Policies:**

Acceptable Use Policy

Internet Policy

Camera and Image Policy

Mobile Technology Policy

Safeguarding Policy

Disciplinary and Grievance Policy

Confidentiality and Data Protection Policy