Beecroft Garden
PRIMARY SCHOOL

BEECROFT GARDEN PRIMARY SCHOOL
ICT MISUSE POLICY

DATE: MARCH 2013

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 breaches of

i. The Acceptable Use Policy
ii. Camera and Image Policy
iii. Internet Policy
iv. Mobile Phone 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 and young people at all times. Should it be suspected at any stage that a child or a 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, 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;

i Children and young people
ii Parents and carers
iii Children Centre staff, Teachers, EYFS Practitioners and support staff
iv Senior Leaders and managers
v Visitors, contractors and community users

3. RESPONSIBILITIES

The Head Teacher (Senior Designated Person for Safeguarding) is responsible for ensuring that the procedures outlined will be followed.

These procedures are to be considered should an allegation of misuse be made against a child, young person or adult.

All ICT users are to be made aware of possible signs of potential misuse. Adults 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 potential sanctions that could be applied should such concerns be raised.

All reports of ICT Misuse must be made directly to the Head Teacher.

4. PROCEDURES

All incidents are to be dealt with on an individual case by case basis.

The context, intention and impact of each incident are to determine the response and actions to be taken. E.g. 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.

Misuse will be categorised as either;

i Minor incident
ii Significant incident
iii Serious incident

Minor Incidents:

- The incident is to be reported to the Head Teacher
- A written incident record is made and the situation 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:

There will always be the possibility that through access to the internet children may gain unintentional access to inappropriate materials. Such material may not be illegal, but it may not be considered suitable in the school setting and / or 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 Head Teacher
- A written incident record is made and the situation monitored.
- 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.
- If the incident relates to inadvertent access to an inappropriate website, this will be banned by Atomwide who provide the internet filters for the school.

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

In respect to misuse by children/pupils, parents and carers will be informed of the alleged incident and advised of any actions to be taken.

Serious incidents:

All serious incidents will be dealt with immediately.

- The incident is to be reported immediately to the Head Teacher
- The context, intention and impact of such misuse must also be considered.
- Appropriate action will be agreed. All details are to be accurately and legibly recorded. The reason why any decision is made will also be noted.
- Should it be considered at any stage that a child is or has been subject to abuse n 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, or volunteer; and there is a suggestion that a child has been subject to any form of abuse, the Safeguarding Policy will again be implemented with immediate effect. The LA Designated Officer must be contacted in the first instance in 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 explicitly requested otherwise by an investigating agency.
- It is 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 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, ipods, ipads, laptops, computers and other portable media technology.
- Internal disciplinary procedures must not be undertaken until investigations by the relevant agencies are completed. Legal and/or HR advise should be sought prior to carrying out any internal and / or instigating high-level disciplinary procedures.
- On completion of both internal and external investigations an online safety review will be undertaken and policies and procedures amended and updated as necessary.

The following incidents must always be reported to the Police immediately, Children's Social Care, Local Authority Designated Officer and Ofsted.

1 Discovery of indecent images of children and young people.
2 Behaviour considered to be 'grooming'.
3 Sending of obscene materials

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

5. MEDIA ATTENTION

Should a serious incident occur, it will most likely attract intense media interest and speculation. On such occasions, every possible attempt will be made to ensure that children and parents/carers are protected from such influences.

An agreed media strategy will be implemented and statements will 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 before any media engagement is undertaken.

Acknowledgements:
Information taken from
Online Safety : A Toolkit for EYFS Settings
Maria Hollett, Plymouth Services for Children and Young People

Online Incident Log Sheet

To be completed as thoroughly as possible by practitioner or manager identifying incident.

Date(s)/ times of incident:
Duration of incident: (**e.g. One off, a week, 6 months etc.)**
Description of the online safety incident: include detail of specific services or websites used (e.g. chat room, instant messenger); email addresses; usernames etc.
Why do you have concerns about this incident?
Has the information been recorded and secured? Yes / No
Has any computer or hardware been secured? Yes / No If yes who, where, when and what?
Who was involved and how do you know this? Is there any evidence to suggest that false names/details have been given? Give full details of real names and email addresses etc where known.

How was the incident indentified? **E.G. by member of staff, informed by third party, identified by IT dept, etc.**

What actions were taken, by whom and why? Give detail of agencies informed and contact person within those agencies.

Name of person completing this form:

Signature:

Department: Children's Centre / Early Years / KS1 / KS2 / Other:

Date :

On completion this form must be passed to the Head Teacher.

Online Safety Incident Log

All online safety incidents must be recorded on the form below. The Head Teacher, working with the ICT coordinator, will be responsible for monitoring incidents regularly, and reporting any concerns or perceived trends to the Senior Leadership Team.

Date / Time	Name of child / Practitioner / other	Computer / Device	Intentional Unintentional Unknown	Details of the Incidents	Actions taken / by whom / when / why	Online Incident Log Sheet completed (Y/N)