BEECROFT GARDEN PRIMARY SCHOOL ACCEPTABLE USE POLICY

DATE: MARCH 2013

1. Aim

The Acceptable Use Policy (AUP) will aim to
- Safeguard children and young people by prompting appropriate and acceptable use of information and communication technology (ICT).
- Outline the roles and responsibilities of all individuals who are to have access to and/or be users of work-related ICT systems.
- Ensure that all ICT users have an acute awareness of risk, a clear understanding of what constitutes misuse and the sanctions that may be applied.

2. Scope

The AUP will apply to all individuals who are to have access to and be users of work-related ICT systems. This will include children and young people, parents and carers, all school and Children Centre staff, managers, volunteers, students, committee members, visitors, contractors and community users. This list is not exhaustive.

Parents / carers and where applicable, other agencies, will be informed of any incidents of inappropriate use of ICT that takes place on-site, and, where known, off-site.

3**. Roles and Responsibilities**

The Head of School is to have overall responsibility for ensuring online safety will be considered an integral part of everyday safeguarding practice.

This will include ensuring;

- All staff and their managers will receive appropriate training, guidance, time and resources to effectively implement online safety policies and procedures.
- Clear and rigorous policies and procedures are to be applied to the use/non-use of personal ICT equipment by all individuals who effect or come into contact with the school / Children's Centre. Such policies and procedures are to include the personal use of work-related resources.
- The AUP is to be implemented, monitored and reviewed regularly, and for ensuring all updates are to be shared with relevant individuals at the earliest opportunity.
- Monitoring procedures are to be open and transparent.
- Allegations of misuse or known incidents are to be dealt with appropriately and promptly, in line with agreed procedures, and in liaison with other agencies, where applicable.
- Effective online safeguarding support systems are in place e.g. filtering controls, secure networks and virus protection.

The Head of School (Designated Person for Safeguarding) will be responsible for ensuring:

- Agreed policies and procedures are to be implemented in practice
- All updates, issues and concerns are to be communicated to all ICT users

- The importance of online safety in relation to safeguarding is to be understood by all ICT users.
- The training, learning and development requirements of all staff are to be monitored and additional training needs identified and provided for.
- An appropriate level of authorisation is to be given to ICT users. Not all levels of authorisation will be the same –e.g. the position/work role/experience.
- Any concerns and incidents are to be reported in a timely manner in line with agreed procedures.
- The learning and development plans of children will address online safety.
- A safe ICT learning environment is to be promoted and maintained.

At Beecroft Garden the Head of School has delegated some of this responsibility to the ICT coordinator.

All School / Children Centre Staff will be responsible for ensuring:

- The timely reporting of concerns in relation to alleged misuse or known incidents, subject to agreed procedures.
- ICT equipment is to be checked before use and all relevant security systems judged to be operational.
- Awareness will be raised of any new or potential issues, and any risks which could be encountered as a result.
- Children and young people are to be supported and protected in their use of online technologies – enabling them to use ICT in a safe and responsible manner.
- Online safety information is to be presented to children and young people as appropriate for their age and stage of development.
- Children and young people will know how to recognise and report a concern.
- All relevant policies and procedures are to be adhered to at all times and training undertaken as is to be required.

All children and young people will be encouraged to:

- Be active, independent and responsible learners, who will contribute as appropriate to policy and review.
- Abide by the Acceptable Use Policy
- Tell a familiar adult about any access of inappropriate content, material that makes them feel uncomfortable or contact made with someone they do not know, straight away, without fear of reprimand (age and activity dependent)

Parents and carers:

- Parents/carers are to be encouraged to sign AUA alongside their children and to share responsibility for their actions and behaviours. This will ensure a consistent message is to be communicated to all.
- A copy of the AUA is to be provided to parents / carers on enrolment of their child at the school. This will be reviewed on an annual basis thereafter. It will be an expectation that parents/carers will explain and discuss the Acceptable Use Agreement with their child to ensure that it is to be clearly understood and agreed. Children will also be encouraged to sign the Acceptable Use Agreement alongside their parent or carer. Records of all signed agreements are to be kept on file.
- Parents / carers will also be required to sign additional Acceptable Use Agreements if they undertake any voluntary work within the school and are to

be given remote access to ICT systems e.g. electronic portfolio or remote webcam.

4. Acceptable use by school / children centre staff and managers.

All staff should be enabled to use work-based online technologies:
- To access age appropriate resources
- For research and information purposes
- For study support

All staff will be subject to authorised use as agreed by the Head of School.

Authorised users will have their own individual password to access the filtered internet provided by the school. Users are generally not permitted to disclose their password to others, unless required to do so by law or where the Head of School has requested. All computers and related equipment are to be locked when unattended to prevent unauthorised access.

All staff are to be provided with a copy of the Acceptable Use Policy and a copy of the Acceptable Use Agreement, which they must sign, date and return. A signed copy is to be kept on file.

The use of personal technologies will be subject to the authorisation of the Head of School, and such use will be open to scrutiny, monitoring and review.

5. In the event of misuse by staff or mangers.

Should it be alleged that a member of staff is to have misused any ICT resource in an abusive, inappropriate or illegal manner, a report is to be made to the Head of School. Should the allegation be made against the Head of School, a report is to be made to the Executive Head Teacher.

Procedures are to be followed as appropriate, inline with the ICT Misuse Procedure, Safeguarding Policies and/ or Disciplinary Procedures.

Should allegations relate to abuse or unlawful activity, Children's Social Care, Ofsted and /or the Police will be notified as applicable.

6. Acceptable use by children and young people.

Acceptable Use Agreements are to be used to inform children and young people of the appropriate behaviours expected to ensure online safety. Children will also be informed of the behaviours which will be deemed unacceptable. This will allow children to take some degree of responsibility for their own actions.

In understanding AUA, children will become aware of the potential risks associated with misuse and the sanctions which will be applied, where necessary.

The AUA are shared and agreed with children and are displayed as a reminder.

7. **In the event of misuse by children and young people.**

Should a child or young person be found to inappropriately misuse ICT the following sanctions will be applied:

- **Step1.**
  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 outlining the issue. The child may be temporarily suspended from a particular activity.

- **Step 2**
  If there are to be further incidents of misuse, the child or young person will be suspended from using the internet or other relevant technology for an increased period of time. The parent/carer will be invited to discuss the incident in more detail with the Head of School 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 & 2 can be omitted. Should a child or young person be considered to be at risk of significant harm, the Safeguarding Policy must be also applied. Allegations of serious misuse will be reported to the most appropriate agency e.g. the Police or Children's Social Care.

In the event that a child or young person should accidentally access inappropriate material, it must be reported to an adult immediately. Appropriate action is to be taken to hide or minimise the window. The computer will not be switched off nor will the page be closed, as it may be necessary to refer to the site during investigations to allow effective filters to be put in place to prevent further inadvertent access.

8. **Acceptable use by parents/carers**

Partnership working with parents/carers should be considered essential practice for promoting an agreed and consistent message which will define acceptable behaviours. Parents and carers will therefore be asked to sign an Acceptable Use Agreement together with their child in order to promote this shared message.

Parents / carers are to be encouraged to contribute to the Acceptable Use Agreement and should be advised to use it should their child access similar technologies at home.

9. **Acceptable use by visitors, contractors and others.**

All individuals who affect or come into contact with the school or children's centre are to be expected to behave in an appropriate and respectful manner. No such individual will be permitted to have unsupervised contact with children. All guidelines in respect of acceptable use of technologies must be adhered to. The right to ask any individual to leave at any time is to be reserved.