BEECROFT GARDEN PRIMARY SCHOOL
INTERNET POLICY

DATE: MARCH 2013

1. Introduction:

The internet should be considered part of everyday life with children and young people seen to be at the forefront of this online generation. Knowledge and experience of information and communication technology (ICT) should be considered an essential life skill. Developmentally appropriate access to computers and the internet in the School and Children's Centre will significantly contribute to children and young people's enjoyment of learning and development.

Children and young people will learn most effectively where they are to be given managed access to computers and control of their own learning experiences; however such use will carry an element of risk. All staff, alongside parents and carers, should consider it to be their duty to make children and young people aware of the potential risks associated with online technologies. This will empower them with the knowledge and skills to keep safe, without limiting their learning opportunities and experiences.

2. Aim

The Internet Policy will aim to outline safe and effective practice in the use of the internet. It will provide advice on acceptable use and effective control measures to enable children and young people and adults tpo use ICT resources in a safer online environment.

3. Scope

The Internet Policy will apply to all individuals who have access to and/be users of work-related ICT systems. This will include children and young people, all staff, managers, volunteers, students, committee members, visitors, contractors and community users. This list is not to be considered exhaustive.

The Internet Policy will apply to internet access through any medium, e.g. Ipods, ipads, laptops, computers, laptops, and PSP's.

4. Responsibilities

The Head of School is responsible for online safety, and will manage the implementation of the Internet Policy.

The Head of School will ensure:

- Day to day responsibility for online safety issues and as such will have a leading role in implementing, monitoring and reviewing the Internet Policy.
- All ICT users are to be made aware of the procedures that must be followed should a potentially unsafe or inappropriate online incident take place.
- Receipt, recording, monitoring and filing of reports should a potentially unsafe or inappropriate online incident occur. This must include the creation of an incident log to be used to inform future online safety practice.
- All necessary actions will be taken to minimise the risk of any identified unsafe or inappropriate online incidents reoccurring.
- Regular meetings are to take place with the Head of School and Senior Leadership Team to discuss current issues, review incident reports and filtering/change control logs.

- Effective training and online safety advice is to be delivered and available to all staff. This should include advisory support to children, young people, parents and carers as necessary.
- Timely liaison, where appropriate, with other agencies in respect of current online safety practices and the reporting and management of significant incidents.

5. Managing online access

a) Password security

Maintaining password security is an essential requirement for all staff. A list of authorised ICT users is to be maintained, and access to sensitive and personal data is to be restricted.

Sharing passwords is not to be considered secure practice.

Pupil passwords are kept on file for reference. (Automatically generated by LGFL).

All ICT users must 'log out' or 'lock' their accounts should they need to leave a computer unattended.

If ICT users should become aware that password security has been compromised or has been shared, either intentionally or unintentionally, the concern must be reported to the Head of School.

b) Internet access

It is to be considered essential practice that internet access for all ICT users will be managed and moderated in order to protect them from deliberate or unintentional misuse. Every reasonable precaution will be taken to ensure the safe use of the internet. It has to be acknowledged however, that it will be impossible to safeguard against every eventuality.

The following control measures will be put in place which will manage internet access and minimise risk:

- Secure broadband and wireless access
- A secure, filtered, managed internet service provider and learning platform
- Secure email accounts
- Regularly monitored and updated virus protection
- A secure password system
- An agreed list of assigned authorised users with controlled access
- Clear Acceptable Use Policies and Agreements
- Effective audit, monitoring and review procedures

In addition:

- Online activity is to be monitored to ensure access will be given to appropriate materials only.
- Computers (and mobile technologies) are to be sited in areas of high visability which will enable children, young people and adults to be closely supervised and their online use to be appropriately monitored.
- All staff are to be made aware of the risks of compromising security, e.g. from connecting personal mobile devices to work-related ICT systems. Such use is to be avoided as far as practically possible. Should, on occasion it be

unavoidable, it will be subject to explicit authorisation by the Head of School. Such use will be stringently monitored.

- Should it be necessary to download unknown files or programmes to any work-related system, it will only be actioned by authorised ICT users with express permission from the Head of School.
- All users are to be responsible for reporting any concerns encountered using online technologies to the Head of School.

c) Online communications

- All official online communications must occur through secure filtered email accounts – LGFL school email.

- All email correspondence will be subject to scrutiny and monitoring.

- All ICT users will be expected to write online communications in a polite, respectful and non-abusive manner. The appropriate use of emoticons is to be encouraged.

- A filtered internet server is used to monitor and prevent offensive material or spam. Should, on rare occasions, security systems not be able to identify and remove such materials, the incident will be reported to the Head of School immediately.

- In line with 'Guidance for Safer Working Practice for Adults who work with Children and Young People' it will not be considered appropriate for staff to engage in personal online communications with children and young people, parents or carers. Express care is also to be taken regarding the use of social networking sites under Principle Eight of the GTC Code of Practice.

- Communications between children and adults by whatever method should take place within clear and explicit professional boundaries. Staff should ensure that all communications are to be transparent and open to scrutiny.

- All ICT users are to be advised not to open emails where they do not know the sender or where the format looks suspicious.

- Online communication is not to be considered private or confidential for safeguarding and security purposes. Such communication is to be monitored and must be available for scrutiny at any time.

- Children and young people will be enabled to use online equipment and resources, when it is to be considered in consultation with parents and carers, that they have the developmental knowledge and understanding to recognise some of the benefits and risks of such communication. Access to online communications will always be monitored by a supervising adult.

- Where children and young people are to access online communications and communities, it will be considered best practice for them to adopt a nickname which will protect their identity and ensure anonymity.

d) Managing multimedia technologies (including Web2 and 3G technologies*)

**Web2 – second generation of web communications e.g. social networking sites*

3G – next generation of mobile/wireless technologies.

Multimedia technologies, where they are used responsibly, will provide easy to use creative, collaborative and free facilities. However, it is to be recognised that there are issues regarding the appropriateness of some content, contact, culture and commercialism.

Ipods, ipads, PSP and mobile phones are equipped with internet access, GPS, cameras, video and audio recording functions. They are therefore considered subject to the same risks as any other form of technology.

Access to social networking sites is restricted and children and young people are only permitted to use moderated child-focused sites under supervision. Staff are not permitted to use work-related technologies for personal access to social networking sites.

Children and young people must always be reminded not to post personal details on websites, particularly information which could identify them or provide information that would contribute to their personal profile, e.g. full name, address, mobile/home telephone number, school details, email address, hobbies/interests.

Children and young people are to be advised on how to set and maintain web profiles to appropriate levels and to deny access to unknown individuals.

Children and young people, parents and carers are to be informed that the use of social networking sites in the home or social environment is to be seen as an exciting communication and networking tool. It must also be emphasised however that their use can pose potential risks. Children and young people, parents and carers should therefore be made aware of the potential risks, and the control measures that can be implemented to minimise them.

It is to be recognised that staff are also likely to use social networking sites in their recreational time on their own personal devices. This form of activity is not to be discouraged however staff must agree and adhere to a 'professional conduct agreement'. It must be ensured that the use of such sites will not compromise professional integrity or bring the school into disrepute. The adding of children and young people, parents and carers as 'friends' to a social networking site should be avoided.

It must be recognised that social networking sites and mobile technologies can be used for negative and anti-social purposes. Cyber bullying e.g. is to be considered as unacceptable as any other form of bullying and effective sanctions must be in place to deal with such concerns. Any known or suspected incidents must be reported to the Head of School immediately.

e) Emerging technologies

Emerging technologies are to be examined to determine potential learning and development opportunities. Their use is to be risk assessed before consideration will be given to enabling use by children and young people. Where necessary, further training and guidance is to be sought to ensure appropriate and safe use of any new technologies.

References:

http://www.dcsf.gov.uk/everychildmatters/resources-and-practice/G00311

General Teaching Council ‘Demonstrate honesty and integrity and uphold public trust and confidence in the teaching profession.