BYRON COURT PRIMARY SCHOOL
Acceptable Use of ICT Systems

1.0 INTRODUCTION

1.1 In recent years the acceptable use of computers in schools has focused on protecting children from the possible dangers presented by the internet. The school has addressed these issues in the school E-Safety Policy.

1.2 This policy will define the acceptable use of ICT resources, networks and systems within the school and set out clear guidelines for all members of the school community. It has been drawn up to protect all parties.

1.3 The school community is defined as all those people (pupils, teaching staff, non-teaching staff, parents, visitors, governors) who engage in learning, teaching, managerial and supportive activities within the confines of the school.

1.4 We are an inclusive school where pupils, parents, staff, governors, the L.A. and local services work in partnership to meet the needs of the community.

1.5 Whilst there are certain key roles for different members of staff, all staff and pupils have a responsibility to ensure that children are safe when using ICT at school. All users have a duty to act in a responsible way to use any ICT equipment within the context of their professional role and to look after the equipment.

1.6 The school strives to overcome barriers to ensure all children have equal access to the National Curriculum whatever their language, culture, gender, physical, intellectual or emotional state and socio economic status.

2.0 AIMS

2.1 Technology will be used in the curriculum to raise standards in teaching /learning.

2.2 The school will ensure that resources will be updated on a regular basis to take advantage of new products and services.

2.3 Children will be taught basic skills and knowledge in ICT to equip them to meet the challenges and changes of our society today and in the future.

2.4 This can be achieved through clear guidelines and procedures in using ICT for all members of the school community.

2.5 The school will ensure that all children have a stimulating and enjoyable learning experience in ICT and using a range of different resources.

3.0 Resources

3.1 These are defined as any form of computing device (for example, servers, work stations, laptops, tablet computers, calculators) irrespective of any form of network connection.

3.2 Any form of peripheral device (e.g. a printer, scanner, video camera, projector, digital microscope) that can be connected to any form of computing device or network connection and is capable of transmitting or receiving or responding to received data.

3.3　Any form of computer or peripheral media, be it fixed or removable (for example, hard disc, CD-ROM memory stick) that can transmit or receive data to or from any form of computing, peripheral or network device.

3.4　Any form of software (e.g. sound programs, appps, image manipulators, data files) that is supplied on or through any form of media or transmission medium.

4.0 Responsibilities

4.1 The principles that are being applied are that all members of the school community should behave at all times within the current legislation and the expectations of the school community.

4.2 Only use school ICT resources to further curriculum. Professional and managerial responsibilities or other uses that are sanctioned by the head teacher, Computing Leader or Chair of Governors.

4.3 Make careful and considerate use of the schools ICT resources, report faults and work in a way that minimizes the risk of introducing computer viruses to the system. The school has also made provision for anti-virus systems to be in place (Sophos Endpoint).

4.4 Protect pupils in school from the harmful or inappropriate material accessible through the internet, or transportable on computer media.

4.5 Support children to use e-mail and similar systems appropriately.

4.6 Recognize responsibility to maintain the privacy of individuals.

4.7 Know and abide by the school's acceptable use policy as it applies to them and people in their care.

5.0 Data Protection and Privacy

5.1 The school will ensure that all stored data is protected from unauthorized access. The children's personal records as well as staff information are kept on a protected specific computer that has limited access to authorized staff only. The information is protected through secure systems that are password protected and maintained by performing backups.

5.2 The school will follow all local and national legislation regarding Data Protection.

6.0 Authorised Use

6.1 The ICT resources are owned by the school and made available to children to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

6.2 The school reserve the right to examine or delete any files that may be held on its computer systems or to monitor any internet sites visited.

6.3 Staff and students using any of the schools ICT resources will sign a copy of the Acceptable User Agreement. There are separate versions for KS1, KS2 and staff. These agreements contain guidelines for the acceptable use of ICT systems within our school.

6.4 All users will be given passwords and security guidelines are outlined in the User Agreements.

7.0 Internet

7.1 We will ensure that all children and staff are protected from illegal and inappropriate materials, as much as possible, by subscribing to a filtered internet provider.

7.2 All children using the internet will be monitored by staff during internet activities and constantly maintain vigilance. This is to safeguard children if protection mechanisms do fail.

7.3 Any user who tries to access inappropriate material will be disciplined through the normal procedures and systems that have been set within the school.

8.0 MANAGING FILTERING

8.1 The school will work with LGFL to ensure systems to protect pupils are reviewed and improved.

8.2 If staff or pupils come across unsuitable on-line materials, the site must be reported to Ilyas Premji (IT technician).

8.3 IT technician will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable- according to LgfL guidelines.

8.4 There is no access to social media sites through the school network.

9.0 Additional Security

9.1 All resources will be security coded with a unique reference which will be recorded in the Asset Management Register (Parago). This will be amended if resources become redundant and are disposed in an authorized manner.

9.2 The school also has alarms fitted to all buildings to protect all resources.

10.0 REVIEW

10.1 Date of policy: December 2017

10.2 Date of review: December 2020