



FINHAM PARK SCHOOL

A Mathematics and Computing College

ICT and E-safety Policy



FINHAM PARK SCHOOL

ICT Usage and E-safety Policy

Policy Date: July 2010 Date of Policy review: July 2011

SECTION ONE: OVERVIEW

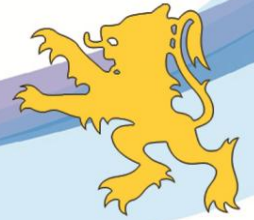
Finham Park School's ICT usage and E-Safety Policy builds upon Becta guidance.

Our policy applies to all students, staff, governors and volunteers associated with the school. The 'staying safe' outcome of Every Child Matters is at the heart of the policy. The 'staying safe' outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for.

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of the school to ensure that every child in our care is safe and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.



1. Current digital technologies

ICT in the 21st century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school include:

- The internet
- Telephone text messaging
- Instant messaging often using simple web cameras
- Social networking sites (Facebook)
- Video broadcasting sites (Youtube)
- Chat rooms
- Blogs
- Podcasting
- Gaming sites
- Music download sites
- File sharing/torrent sites
- Mobile phones with camera and videos
- Games consoles with internet communication
- Smart phones with e-mail and web functionality.

2. E-Safety Risks

The risks can be summarized under the following headings as identified in Becta's report "Safeguarding Children in Digital World" (2006)

2.1 E- Content

- Exposure to age inappropriate material – pornography, etc.
- Exposure to inaccurate or misleading information
- Exposure to socially unacceptable material, such as that inciting violence, hate or intolerance.

2.2 E-Contact

- Grooming using digital communication leading to sexual assault.

2.3 E-Commerce

- Exposure of minors to inappropriate commercial advertising
- Exposure to online gambling
- Commercial and financial scams .



2.4 E-Culture

- Bullying via mobile phones/social networking/websites or other forms of digital communication including untruthful, hurtful and abusive comments or imagery
- intended to denigrate or humiliate another
- Illegal downloading of copyrighted materials , i.e. music and films.

3. Strategies to minimize e-safety risks

- E-Safety classroom displays in and around ICT classrooms
- E-Safety taught to all students through Year 7 ICT curriculum
- Guidance on tackling cyber bullying through pastoral programme
- Sanctions covering use of ICT, through the school's behaviour for learning policy
- Log on screen for all students has a tick box indicating acceptance of the school internet policy
- Filtering systems to prevent access to inappropriate material internal ZyXel hardware filtering and Redstone external filtering)
- Use of Altman P-Counter software to intercept documents with offensive or inappropriate content before they are printed
- Policy Central software (automatically generates screen grabs from pupils' screens when potentially offensive or inappropriate words are detected)
- Surveillance software (Synchron-Eyes) monitoring all PC use within the school
- CCTV installed in computer rooms
- Child protection issues reported to the Deputy Head Teacher responsible for Child Protection
- E-Safety concerns are reported direct to the Subject Leader for ICT and, where appropriate, the Deputy Head Teacher.

4. How complaints regarding E-safety will be handled

The school will take all reasonable precautions to ensure E -Safety. However, owing to the global scale and linked nature of internet content, the wide availability of mobile and digital technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of internet access.

SECTION TWO: STAFF/PUPIL USAGE POLICIES

1. PUPIL USAGE

The computer network is owned by the school and is made available to students to further their education. The school's Computer and Internet Acceptable Use Policy has been drawn up to protect everyone and failure to comply with this policy will result in students not being able to use school computers or more serious sanctions in accordance with the Finham Park School's Behaviour for Learning system.



Use of the school computer system:

- I will use the school's computers for school related study purposes only
- I will only use my own username and password and I will keep my password secret
- I will ensure that I log off when I have finished using the computer
- I will not eat or drink near a computer
- I will treat the school computers and computer equipment with care and respect and I accept that I will be expected to pay for any damage caused by careless use or deliberate abuse
- I will not attempt to install any software or re-arrange the hardware
- I am responsible for the files stored in my network areas and it is up to me to keep a back up of any work which might be important
- I understand that the school will check my files and monitor the sites I visit

Use of the internet and email

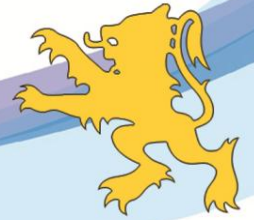
- (Unless I have specific permission in a specific lesson for a reason decided by a member of staff) - I will not enter chat rooms, play internet games or access social networking sites
- I will use the internet to help me with me with my school work. I will only enter sites that I have a teacher's permission to enter
- I will not use the internet to find information and then submit it as my own work
- I will access or attempt to download content which would be deemed inappropriate or offensive
- My emails will be polite and sensible. I will communicate with others by email in a way that reflects the **rights and responsibilities** of other members of Finham Park.
- I will not give out any personal information [like my mobile number, address] online or in emails. I will not arrange to meet anyone that I do not know.

I accept that if I break any of these rules I may be stopped from using the school's computers

Some behaviours can be deemed serious to warrant immediate issuing of a C3/C4 under the behaviour for learning.

B4L warranting immediate C3's/C4's

- Damage to computers or hardware (including headphones, mice, pulling out leads etc)
- **[immediate C4 under the new B4L system]**
- Turning off someone else's PC
- **[immediate C3 under the new B4L system]**
- Inappropriate internet access (for offensive content as opposed to games or just being off task)



- **[immediate C4 under the new B4L system]**
- Use of email or computer for bullying (posting comments or sending unpleasant emails)
[immediate C4 under the new B4L system]

Students receiving C4's will have additional sanctions, depending on the nature/severity of the offense and whether or not this is a first offense

Stage 1

- Network Ban (discretionary, determined by Subject Leader for ICT)
- Phone call/ Letter Home
- Learning Conversation with Subject Leader of ICT to discuss behaviour

Stage 2 [second offense]

- Network Ban
- Contact home and meeting with Parent/Progress Leader

Stage 3 [third offense]

- LT involvement

2. Staff Usage Policies

These are divided into two key areas;

I. Staff use of laptops

II. Staffs use of school computer rooms

I. LAPTOP USAGE

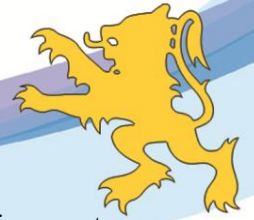
- Staff use of school laptops for internet and email, is covered by the **School Email and Internet Protocol/Policy**.
- General usage is covered by the **Laptop agreement**.
- Staff who have not been issued with a school laptop and who use personal ICT equipment in school, are expected to abide by the guidelines of the above policies

In addition to this:

- Staff should understand the student policy and ensure that this upheld when they are responsible for students using ICT
- Staff should ensure that they do not allow students to use ICT

II. STAFF USAGE OF ICT ROOMS

PLEASE ENSURE THAT:



- You are fully conversant with the aspects of the school's Behaviour for Learning system relating to use of ICT
- Students are told to wait outside the room until you arrive
- Work printed by students is not left on desks
- Before printing students have:
 - Spell-checked their work
 - Used "Print Preview" to ensure that the work print as expected
 - Selected the correct printer for the room
 - Ensure that their name is on their work
- Headphones (if used) are disconnected and returned. None should be left out at the end of the lesson and students are on no account allowed to take them out of the room
- Students are logged off at the end of the lesson
- Chairs are left behind desks at the end of the lesson
- Air conditioning/fans are turned off (if used) at the end of the lesson
- All materials/equipment brought to the room, such as folders, text books, exercise books, worksheets) are removed at the end of the lesson
- All pupils are carefully monitored at all times and any damage/misuse is reported
- Students do not eat or drink in the classroom

For teachers using a room in Period 5:

- Please ensure that the LCD projector is turned off at the end the lesson
- Please ask students to shut down their machines at the end of the lesson



ICT & E-SAFETY POLICY

Written by J Bridgeman on:
Review date:

July 2010
July 2011

Approved by Governors:

28 September 2010

Signed:

A handwritten signature in black ink, appearing to read 'Mark Bailie', is written over a horizontal line.

MARK BAILIE
Headteacher

Date:

Signed:

A handwritten signature in black ink, appearing to read 'Peter Burns', is written in a cursive style.

PETER BURNS
Chair of Governors

Date: