FINHAM PARK SCHOOL
A Mathematics and STEM College

Computing and E-safety Policy

SECTION ONE: Overview

Finham Park School's Computing usage and E-Safety Policy builds upon the GDPR.

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 Computing 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 Computing 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.

Computing and Computing also continues to have a significant impact on us whether it be at school, home or work. It is therefore important that pupils achieve a good level of technical understanding and teachers themselves are supported through our CPD.

1. Current digital technologies

Computing 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 can include:

- The internet
- Telephone text messaging

- Instant messaging often using simple web cameras
- Social networking sites (Facebook, Twitter, WhatsApp, Messenger, Instagram, Tumblr, TikTok, Reddit)
- Video broadcasting sites (Youtube)
- Chat rooms
- Blogs
- Podcasting
- Gaming sites
- Music download sites
- File sharing/torrent sites
- Email on all platforms
- Mobile phones with camera and videos
- Games consoles with internet communication
- Tablets and smart phones with web functionality.
- Virtual Learning Environments (VLE's)
- Virtual reality goggles\headsets
- Video conferencing
- Screen capture video
- Flipped learning video

2. E-Safety Risks

The risks can be summarized under the following headings:

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
- Exposure to extremist material or propaganda

2.2 E-Contact

- Grooming, including the use of digital communication leading to all forms of sexual contact
- The use of digital technology to either create or distribute images of a sexual nature for the purpose of blackmail is a criminal offence and will be treated accordingly

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 intended to denigrate or humiliate another member of the school community
- Illegal downloading of copyrighted materials, i.e. music and films.
- The school regards torrenting or file sharing of copyrighted material as a criminal offence and this will be dealt with accordingly.
- Fake news

2.5 E-Video Conferencing

- Hijacking of meetings which can be disruptive and disturbing for participants
- Recordings of meetings without prior agreement.

3. Strategies to minimize e-safety risks

- E-Safety classroom displays in and around Computing classrooms
- Annual participation in Safer Internet Day
- E-Safety taught to all students through the Computing and PSHRE curriculum
- Guidance on tackling cyberbullying through the pastoral programme
- Sanctions covering the use of Computing, 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 (Smoothwall)
- Use of Papercut software to intercept documents with offensive or inappropriate content before they are printed
- Lan School software (automatically generates screen grabs from pupils' screens when potentially offensive or inappropriate words are detected)
- Surveillance software (Smoothwall) 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 directly to the Subject Leader for Computing and, where appropriate, the Deputy Head Teacher
- Updates and training for all staff
- For video conferencing: -
    - Use waiting room features (therefore controlling who enters the room)
    - Passwords are used (most applications are now starting to implement this feature) and by default, there should be a meeting number
    - Control sharing (some applications allow this feature)
    - Provide links directly to participants
    - Lock the meeting once all is present.

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. Also, the school cannot account for the range of viruses that may cause damage to the 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 is contingent upon:

- Use of the school's computers for school related study purposes only
- Using their own username and password and keeping personal passwords secret
- Logging off when finished using the computer
- Responsibility for personal "Frog" and Google Drive accounts and all usage that happens under any login
- Not eating or drinking near a computer
- Treating the school computers and computer equipment with care and respect at all times and accepting that there will be an expectation to pay for any damage caused by careless use or deliberate abuse
- Not installing or attempting to run any software (on the main computer system or via external hard drives) or re-arranging the hardware under any circumstances.
- The use of proxy un-blockers or similar system to re-route web traffic is strictly forbidden.
- Taking responsibility for the files stored in personal network areas and keeping a back-up of any work which might be important
- Accepting that the school will check personal files and monitor the sites visited

Use of the internet and email (including use of the school's VLE "Frog" & Google Classroom)

- Use of chatrooms, games, social networking sites and playing internet games without the explicit permission of the supervising member of staff is strictly forbidden.
- The internet will be used to help with school work. Students will only enter sites that they have a teacher's permission to enter
- Students will not use the internet to find information and then submit it as their own work, in accordance with the JCQ policies on Controlled Assessments and Coursework, and On-screen tests
- Students will not access or attempt to download content which would be deemed inappropriate or offensive
- Emails and social media communication will be polite and sensible. Communication with others by email should reflect the **rights and responsibilities** of other members of Finham Park community.
- Students must also ensure that they behave responsibly when using Frog, Google Classroom or virtual classrooms and use it appropriately at all times (whether posting status updates, messaging, emailing or making use of forums)
- Students will not give out any personal information [like my mobile number, address] online or in emails. They must **never** arrange to meet anyone that they do not know.
- Create, transmit or cause to be transmitted any material which is vulgar, obscene or contains sexually or racially explicit language or material.

Some staff or students may use their own mobile devices which are 5G enabled and which can therefore access online content which cannot be monitored or restricted through the school's filtering system.

The following principle applies in this case:

- The school's rules regarding the accessing of inappropriate material (covered in 2.1 – 2.4) apply regardless of whether students are using the internet provided via the school service or mobile data provided via a 3rd party.

Any breach of these rules may result in the removal of privileges in the use of the school's computers. Some behaviours can be deemed serious to warrant immediate issuing of a C3/C4 under the behaviour for learning.

2. Use of mobile technology (Bring your own devices - BYOD)

SMART learning is the use of mobile technology in order to access and leverage the power of internet materials, videos etc for the purposes of engaging and stretching learning.

- It is our intention that students will be able to access learning material via mobile devices in school at the discretion of teachers, subject leaders and pastoral leaders.
- It is the responsibility of all members of the school community to keep all passwords safe at all times
- Access to the school wifi may be rescinded in cases of inappropriate use
- USB drives may be connected to School computers if needed, to upload and download work, but it is preferable to use the Google Classroom or FROG for this purpose. It is the responsibility of the student that any USB drives used on the School computers have been scanned for viruses. The IT technical Department can help with this.
- See document on BYOD

3. Use of Social Media

Rationale

The widespread availability and use of social media applications bring opportunities to understand, engage, and communicate in new and exciting ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our duties to our school, the community, our legal responsibilities and our reputation.

For example, our use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults. The policy requirements in this document aim to provide this balance to support innovation whilst providing a framework of good practice.

They apply to all members of staff at the school. The purpose of this part of the policy is to:

- Protect the school from legal risks
- Ensure that the reputation of the school, its staff and governors is protected
- Safeguard all children
- Ensure that any users are able clearly to distinguish where information provided via social media is legitimately representative of the school.

Definitions and Scope

Social networking applications include, but are not limited to: Blogs, Online discussion forums, Collaborative spaces, Media sharing services, 'Microblogging' applications, and online gaming environments. Examples include Twitter, Facebook, Windows Live Messenger, Reddit, Instagram, Snapchat, WhatsApp, LinkedIn, YouTube, Flickr, Xbox Live, Blogger, Tumblr, Last.fm, and comment streams on public websites such as newspaper site.

Many of the principles of this policy also apply to other types of online presence such as virtual worlds.

All members of staff should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, GDPR and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation.

They must also operate in line with the school's Equalities, Child Protection and ICT Acceptable Use Policies.

Within this policy there is a distinction between use of school-sanctioned social media for professional educational purposes, and personal use of social media.

SECTION THREE: Use of Social Media in practice

1. Personal use of social media

• School staff will not invite, accept or engage in communications with parents or children from the school community in any personal social media whilst in employment Finham Park School.

• Any communication received from children on any personal social media sites must be reported to the designated person for Child Protection/

• If any member of staff is aware of any inappropriate communications involving any child in any social media, these must immediately be reported as above

• Members of the school staff are strongly advised to set all privacy settings to the highest possible levels on all personal social media accounts

• All email communication between staff and members of the school community on school business must be made from an official school email account

• Staff should not use personal email accounts or mobile phones to make contact with members of the school community on school business, nor should any such contact be accepted, except in circumstances given prior approval by the Head Teacher.

• Staff are advised to avoid posts or comments that refer to specific, individual matters related to the school and members of its community on any social media accounts

• Staff are also advised to consider the reputation of the school in any posts or comments related to the school on any social media accounts

• Staff should not accept any current pupil of any age or any ex-pupil of the school under the age of 18 as a friend, follower, subscriber or similar on any personal social media account

• Staff should regularly check their privacy settings as this is sometimes reset.

2. School-sanctioned use of social media

There are many legitimate uses of social media within the curriculum and to support student learning. For example, the school has an official Twitter account (@finhampark), and several departments make use of Twitter to provide support the learning of their students by raising engagement in the subject, providing access to learning and revision materials and also providing support during exam seasons. Some departments make use of YouTube as a way of recording assessed work – for instance videoed presentations – so that this may be viewed by visiting exam moderators. This has been identified as an example of good practice by examination boards. The are many other possibilities for using social media to enhance and develop students' learning.

When using social media for educational purposes, the following practices must be observed:

• Staff should set up a distinct and dedicated social media site or account for educational purposes. This should be entirely separate from any personal social media accounts held by that member of staff, and ideally should be linked to an official school email account.

• The URL and identity of the site should be notified to the appropriate Head of Faculty or member of the SLT before access is permitted for students

• The content of any school-sanctioned social media site should be solely professional and should reflect well on the school.

• Staff must not publish photographs of children without the written consent of parents / carers, identify by name any children featured in photographs, or allow personally identifying information to be published on school social media accounts

• Care must be taken that any links to external sites from the account are appropriate and safe

• Accounts must be monitored regularly and frequently (preferably several times a week, including during holidays). Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

• Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.

- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.
- We aim to promote positive relationships and the effective use of social media platforms that keep stakeholders informed on updates regarding the school. The school recognises the potential benefits of social media but is aware of the potential harm it can also cause to individuals.
- We aim to avoid the promotion of untrue reports and encourage our followers to be mindful of untrue reports. Any account making comments that may be deemed offensive to an individual within the school community, inciting hatred or bringing the school into disrepute on the school social media forums will be reported to the relevant body and the account blocked.
- Any account raising a discussion point on social media is free to make an appointment to discuss in person at the school. The school will not engage in public discussions over social media.

SECTION FOUR: Cloud based applications and services.

1. Using Online data and cloud storage

There are many opportunities for staff and students to take advantage of an increasingly wide and diverse range of cloud based (online) tools and services. These include “web applications” and online software packages that provide students with access to content creation. These include, but are not exclusive to, Powtoon (an online package that allows students to animated presentations, Animito (an online video creation tool) and Draw.io (an online diagram/flowchart maker), Eedi (an online collection of computing quizzes))

- Many such services require users to register before access is granted and staff should be **wary about the use of any website that requires students to provide personal information, or register by way of a social networking service such as Facebook or Twittter.**
- Finham Park is a Google Apps for Education school. This means that every member of staff has access to Google Services via an account provided and managed by the school.
- School Google accounts provide students with a login that does not necessitate them to provide any personal information whatsoever
- Many cloud services allow users to sign up/register via a Google account.
- Staff should ensure that online/cloud-based tools are restricted to services that support Google sign-in. This would ensure that students could register for the service without sharing any personal information.

- There may be exceptions to this – such as ucas.com – where personal data is required. Staff should contact the Head Teacher or the Head of Faculty for Computing if unsure.

B4L warranting immediate C3's/C4's

- Damage to computers or hardware (including headphones, mice, pulling out leads etc)
  [Immediate C4]
- Turning off someone else's PC
  [Immediate C3]
- Inappropriate internet access (for offensive content as opposed to games or just being off task)
  [Immediate C4]
- Use of email or computer for bullying (posting comments or sending unpleasant emails)
  [Immediate C4]
- Use of Frog for posting inappropriate/offensive material (via forums, status updates, messages or emails), or for cyber bullying
  [Immediate C4]

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

Stage 1

- Network Ban (discretionary, determined by Subject Leader for Computing)
- (When appropriate) VLE ban (discretionary, determined by Subject Leader for Computing/E Teaching Staff/LT)
- Phone call/ Letter Home
- Learning Conversation with the Subject Leader of Computing to discuss behaviour

Stage 2 [second offence]

- 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\computers

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.**
- Staff will be assigned a password that will be securely recorded by IT Services. Staff will no longer be able to have the ability to alter this. Each password is completely unique. Any devices that use school services such as Outlook for mobile, will require your new password to be entered to continue working.
- Laptops will require Windows 10, and by law will require software encryption which will be arranged by the IT Team
- All memory sticks must use software encryption
- General usage is covered by the **Laptop agreement**
- Staff who have not been issued with a school laptop and who use personal Computing 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 is upheld when they are responsible for students using Computing
- Staff should ensure that they do not allow students to use their own staff laptops under any circumstances.

II. STAFF USAGE OF COMPUTING ROOMS

Staff are responsible for the behaviour of students whilst using school computers. All colleagues are expected to be vigilant and ensure that students are fully supervised at all time. Specific rules for usage are provided below, but these can be summarised simply with the expectation that staff should **leave Computing rooms in the condition that they would expect to find them**. Specifically;

PLEASE ENSURE THAT:

- You are fully conversant with the aspects of the school's Behaviour for Learning system relating to use of Computing

- No equipment is altered, reconfigured or disconnected for any purpose – Where a ceiling-mounted projector is connected to a desktop computer, staff must not disconnect the projector in order to connect their own laptops. If in doubt, advice should be sought from ICT Tech.
- Requests for additional or "special" equipment that requires technical support are logged with ICT Technicians at least 48 hours in advance. This needs to be emailed to support@finhamparkmat.co.uk
- Students should never enter a Computing classroom without a member of staff present
- Work printed by students is not left on desks

  Before printing students have:

  - o Spell-checked their work
  - o Used "Print Preview" to ensure that the work print as expected
  - o Selected the correct printer for the room
  - o Ensure that their name is on their work

- **Headphones (if used with permission from supervising staff) 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, textbooks, exercise books, and 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
- Personal Student Data (such as SEN or disadvantaged student information) is not displayed while a laptop is connected to a projector.
- Staff have filled in the Google Forms survey after using an IT room to confirm the room has been checked for the above and any damage is reported to Head of Department and IT services by emailing support@finhamparkmat.co.uk (this will automatically log a request for any issues to be looked into).

For teachers using a room in Period 5:

- Please ensure that the projector and TV are turned off at the end the lesson
- Please ask students to shut down their machines at the end of the lesson.

FINHAM PARK SCHOOL
A Mathematics and STEM College

COMPUTING & E-SAFETY POLICY

Written by J Bridgeman on:	July 2010
Review date:	July 2011
Review date:	July 2012
Review date:	July 2013
Review date:	May 2015
Reviewed by J Bridgeman	October 2016
Reviewed by N Powell	Nov 2018
Reviewed by N Powell	May 2020
Reviewed by S Mahmood	November 2022
Next Review Date:	January 2025

Signed:

Mr Chris Bishop

Headteacher

Date: January 2023

Signed:

Ms Mandy Gilmore

Chair of Governors

Date: January 2023