Royal Borough of Kingston upon Thames

Green Lane Primary and Nursery School

# The Coombe Academy Trust
# ESafety Policy

## 1. Introduction and Overview

### The purpose of this policy is to:

- Outline the guiding principles for all members of the school community regarding the use of ICT.
- Safeguard and protect the students and staff and help them to work safely and responsibly with the Internet and other communication technologies.
- Set clear expectations of behaviour relating to responsible use of the Internet for educational, personal or recreational use.
- Establish clear reporting mechanisms to deal with online abuse such as bullying that are cross referenced with other school policies.
- Ensure that all members of the school community know that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

### Scope of the policy

This policy applies to all members of school community - staff, students, volunteers, parents and carers, visitors, community users and anyone else who have access to and are users of school's ICT systems.
ICT system is defined by any system or device that is provided by the school. This includes but is not limited to:

- School-owned PCs and devices available for use on-site (e.g. desktop PCs)
- School-owned devices that are taken off site (e.g. laptops)
- Any device (personal or school-owned) connected to the network (including wireless) are bound by this policy and the Acceptable Use Policy while connected
- Online services, e.g. Office365 (email, OneDrive, etc), Google Apps (Drive, Classroom, etc), Insight, PARS and other school-managed services available inside and out of school and from school-owned or non-school owned devices
- Remote Access from staff own devices, any device connected to the school network via remote access is bound by this policy and the Acceptable Use Policy while connected

### Communication of the policy

The policy will be communicated to the school community in the following ways:

- Displayed on the school website, and available in the staffroom and classrooms
- Included as part of the induction pack for new staff and included in staff handbook, Acceptable use agreements are included in the home-school agreement which parents sign upon entry to the school
- Acceptable use agreements to be held in student and personnel files
- Acceptable use policy is shown to staff and students upon logon to the network

### Responding to complaints

- The school will take all reasonable precautions to ensure eSafety. However, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor CSSAT can accept liability for material accessed, or any consequences of Internet access.

- Staff and students are informed of the possible sanctions related to misuse of technology and these are outlined in the Behaviour Policy and Acceptable Use Policies.
- Any eSafety concern should be taken to the Esafety Coordinator or Director of IT.
- Any complaint about staff misuse will be referred to the Headteacher.
- Complaints that relate to online bullying will be dealt with in line with our Anti-Bullying Policy. Complaints related to child protection are dealt with in line with the school child protection procedure.

### Review and Monitoring

ESafety is integral to other school policies including the Child Protection Policy, Anti-Bullying Policy and Behaviour Policy.

The school's eSafety coordinator is responsible for writing, reviewing and updating the policy. The policy will be reviewed annually or more frequently in response to changing technology and eSafety issues in the school.

This policy has been developed in consultation with the school's eSafety committee and approved by the Senior Leadership Team and Board of Governors. Staff will be informed of any updates or amendments to it.

## 2. <u>Education and Curriculum</u>

### Student eSafety curriculum

The school has a clear, progressive eSafety education programme primarily as part of the Computing curriculum / PSHE curriculum but referenced in all areas of school life. It covers a range of skills and behaviours appropriate to students' ages and experience, including:

- Digital literacy
- Acceptable online behaviour
- Understanding of online risks
- Privacy and security
- Reporting concerns

Students are taught to think carefully about placing any personal photos on social media sites. The importance of privacy settings as a tool to safeguard their personal information is included in eSafety education. They are also taught that they should not post images or videos of others without their permission.

Students understand the risks associated with sharing images that reveal the identity of others and their location, such as house number, street name or school.

The school will:

- Plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Remind students about their responsibilities using the Acceptable Use Policy.
- Ensure that staff model safe and responsible behaviour in their own use of technology during lessons.

- Ensure that staff and students understand issues around plagiarism and copyright/intellectual property rights, and understand how to critically assess the validity of the websites they use.

### Staff and governor training

The school will ensure that:

- Staff understand the requirements of the Data Protection Act in terms of sending and receiving sensitive personal information.
- Regular training is available to staff on eSafety issues and the school's eSafety education programme.
- Information and guidance on the eSafety policy and the school's Acceptable Use Policy is provided to all new staff and governors.

### Parent engagement

The school recognises the important role parents and carers have in ensuring children and young people are safe, responsible and can flourish online.  To support parents to understand online risks and the work of the school in this area we will provide:

- Acceptable Use Agreements to all new parents.
- Regular, up to date information in newsletters and on the website and social media, particularly in response to emerging trends.
- Face to face sessions in school.
- Opportunities to share in their children's eSafety learning (eg assemblies, performances).
- Support and advice on online safety for their children outside of school.
- Signposting to further resources and websites.

## 3. Conduct and Incident management

### Conduct

All users are responsible for using the school ICT systems in line with the Acceptable Use Policy they have agreed to by accepting the terms upon login.  They should understand that there will be consequences of misuse or access to inappropriate materials which may result in sanctions for pupils in line with the school's Behaviour Policy.

All members of the school community should know that this policy also covers their online activity outside of school if it relates to their membership of the school.

Parents and carers will be asked to give consent for their children to use the internet and other technologies in school, by signing an Acceptable Use Agreement.  They will also be given clear information about the sanctions that might result from misuse.

### Social Media

The Child Protection Policy sets out the requirements for staff in the appropriate use of their personal social media accounts. The use of school social media accounts (e.g. for marketing) is managed by a nominated member of staff with guidance from the eSafety Coordinator.

## Incident Management

All members of the school community understand they have a responsibility to report issues and are confident that anything raised will be handled quickly and sensitively. Anyone who is concerned about the safety of a child should report concerns to the Child Protection Officer immediately. The school actively seeks advice and support from external agencies in handling eSafety issues. Parents and carers will be informed of any eSafety incidents relating to their own children.

## 4. Managing the ICT infrastructure

The school is responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible and that related policies and procedures are implemented. It will also ensure that the relevant people will be effective in carrying out their eSafety responsibilities with regards to the ICT infrastructure.

- The technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of the school's technical systems.
- All users will have clearly defined access rights to the technical systems and school owned devices.
- All users will be provided with a username and secure password. Users will be responsible for the security of their username and password.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes managed by the IT Support department.
- The school allows different filtering levels for different groups of users – staff, students and IT support. Specialist subjects, e.g. Media Studies have filtering policies to allow access to more open websites such as Youtube and blog sites. This is limited to the subject area and managed by the head of department.
- The school regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- There is a reporting system in place for users to report any technical incident or security breach. Staff are expected to log all technical issues on the online helpdesk system.
- Security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. Secure online storage and remote access systems are provided for staff access outside of school.

## 6. Data

The school has a Data Protection Policy that is regularly reviewed and updated. This includes information on the transfer of sensitive data; the responsibilities of the Senior Information Risk Officer; and the storage and access of data.

## 7. Equipment and Digital Content

### Personal mobile phones and mobile devices

Personal mobile phones and mobile devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personal mobile phones or mobile devices. The use of staff personal devices is outlined in Appendix 3 - Staff Personal Device & Remote Access Policy.

### Staff Use

The use of staff mobile phones is outlined in Appendix 3 - Staff Personal Device & Remote Access Policy.

### Digital images and video

The school's use of images and videos of students is outlined in the Images and Videos Parental Consent.

Students are taught to think carefully about placing any personal photos on social media sites. The importance of privacy settings as a tool to safeguard their personal information is included in eSafety education. They are also taught that they should not post images or videos of others without their permission.

Students understand the risks associated with sharing images that reveal the identity of others and their location, such as house number, street name or school.

Appendix 1 - Pupil Acceptable Use Policy

# All pupils will:

- Use the ICT facilities to aid and enhance their learning
- Protect themselves by:
    - Using only their personal login and keep the password secret
    - Logging off when not using the computers to protect their data
    - Using email and VLE messaging systems in a responsible manner
    - Not going on websites or programs not relevant to the lesson objectives
    - Not attempting to access any site or materials that are blocked by the web filter
    - Not using any communication system apart from the school-provided email and VLE messaging system (including, but not limited to social networking sites, chatrooms, non-school email and instant messaging systems)
    - Not using email or VLE messaging to make unsolicited contact with unknown users
    - Not sending any inappropriate content via email or VLE messaging
- Protect the network by:
    - Respecting the ICT equipment
    - Reporting any damage to the equipment to a member of staff as soon as it is discovered
    - Reporting any inappropriate material discovered while using the ICT equipment to a member of staff immediately so that it can be investigated
    - Not using anyone else's username and password
    - Not attempting to install software or alter computer settings
    - Not connecting any non-school-owned equipment to the school network without explicit permission from the ICT support team
- Obey the LGFL acceptable use policy when using LGFL services.

**NOTE: If you do not abide by these rules, your access may be limited or revoked**

## Appendix 2 - Staff Acceptable Use Policy

# All staff will:

- Use the ICT facilities to aid and enhance their teaching and pupils' learning
- Protect pupils by:
    - Educating pupils about responsible use of computers and the internet
    - Reporting any inappropriate material discovered while using the ICT equipment to the ICT support team
    - Using classroom monitoring software to control and monitor ICT use during lessons
    - Reporting any misuse of ICT facilities to relevant SLT
- Protect data by:
    - Logging off when not using the computers
    - Keeping their password secret
    - Not transferring sensitive or confidential data onto memory sticks, other removable media or laptops unless encrypted by the ICT support department
- Protect the network by:
    - Report any damage to the equipment the ICT support team as soon as it is discovered
    - Not attempt to access any site or materials that are blocked by the web filter
    - Not attempt to install software or alter computer settings
- Protect themselves by:
    - Not communicating online with pupils via social networking sites or other online mediums which are not sanctioned by the school.
    - Obey the LGFL acceptable use policy when using LGFL services.
    -

**NOTE: If you do not abide by these rules, your access may be limited or revoked**

## Appendix 3 - Staff Personal Device & Remote Access Policy

# Staff Personal Device & Remote Access Policy

### Introduction

This policy explains the rules and guidelines for staff using personal devices at school (often known as BYOD or 'bring your own device').

Using your own device in school raises some data security and eSafety issues. The school is responsible for school data that you process on personal devices. You should always treat personal information with great care and keep it as secure as possible. If you use your own device for school work you will need to ensure that you meet the school's responsibilities for data handling, which includes allowing access to your personal device if necessary.

If you want to use a personal electronic device in school, you must have the agreement of your manager. We may have to refuse some access requests for security reasons.

### Using Personal Devices in School

Staff may wish to bring their own devices to use in school. There are several considerations that need to be taken when using personal devices on site.

### Health & Safety

Any electrical devices, particularly devices requiring mains power must be certified to be safe. This means that the device and/or power cable/adaptor must be inspected or PAT tested by the site manager before use as set out in the Health and Safety Policy Appendix 27 – Premises and Work Equipment.

### Insurance

The schools' insurance will not cover personal devices that are on site. The school will not be held responsible for any loss or damage to personal devices. Personal devices should not be left on the school site overnight.

### Acceptable Use Policy

Personal devices that are connected to the school network through WiFi, remote access or any other means are subject to the same web filtering and security policies that apply to the school PCs. By connecting any personal device to the school network, that device is subject to the ICT Acceptable Use Policy.

### Security

The school has responsibility under the Data Protection Act to ensure "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data." This principle extends to data stored on personal devices and additional precautions must be taken on personal devices as the risk of data loss is greater due to the portable nature of devices.

Some school data is highly sensitive and should never be stored on a personal device. If you are unsure about what information can be stored or the protections you should use, you should ask for guidance from your line manager or the data protection officer.

### Device Security

Any device that stores personal data must be protected by the following:

Lock Screen Pass-codes/passwords

Devices must be set to automatically lock after a period of time. The lock-screen must be protected with a password or pass-code with a minimum length of 4 digits. The device should automatically block or wipe itself after a certain number of failed attempts to unlock.

Device Encryption

The devices must be encrypted. This is more comprehensive protection than just having a password/code, as without encryption the security can be easily bypassed. Most modern devices support encryption as standard, please refer to the operating instructions for your particular device to enable it. Contact IT Support if assistance is required.

Remote lock & wipe

The devices must have a mechanism for the user or the school to remotely lock and wipe the contents of the device if it is lost or stolen. This can be achieved through the school email system if the device has a school email account set up.

## Device Control Policies (MDM)

The school can enforce these policies by enrolling devices in a Mobile Device Management (MDM) system. This involves installing an app on the device which then applies certain policies to the device. The app will report certain information about the device back to the school. This includes information about the identity of the device (manufacturer, model number and serial number), the security capabilities of the device (whether encryption and passcodes are enabled) and allow the school to erase the contents of the device or locate it using GPS if it is lost or stolen. It is the choice of the device owners whether to allow the school to activate MDM on the device, but the school may block access certain services from devices that are not enrolled in MDM.

## Loss and Theft

If your personal device has been used for school business and is lost or stolen, you must report the incident to the school's IT Services Team as soon as possible. The IT Services Team will take steps to ensure the security of school data, and this may include a remote wipe of data (removing all school data from your device). This may result in the loss of any personal information stored on the device.

## Process for Dealing with Loss or Theft of Personal Device

When the IT Support Team is notified of a lost or stolen device which may contain personal data they will follow the following process:

1. Inform the Director of IT to log the incident.
2. Guide the user through changing their password for all school systems.
3. Use the Exchange or Office 365 to send a remote-wipe command to the device. Please note: this will permanently remove all data on the device: school data and personal data.
4. Check access logs to see if any potential data breach may have occurred. If it is suspected that data-loss has occurred, the case will be escalated and the procedure in the Data Protection Policy will be followed.

## Methods of Accessing School Data from Personal Devices

### Email

Email accounts can be added to mobile devices, either through the device's native email app or using the Outlook mobile app. As these methods store data locally on the device, the security policies must be adhered to. The Outlook app and built-in email on most mobile devices can be secured with the school MDM. The full desktop version of Outlook cannot be secured in the same way and therefore **should not be used on personal devices including laptops and home PCs without suitable protection: encryption and strong passwords.** When Outlook is installed on school-owned staff laptops they should be encrypted and secured by the IT department.

### Files

In the past, staff members used to take files off site on USB drives and external hard drives to work on at home. **This is an extremely insecure way of transporting school data and should not be used.** The school provides other means to work on files outside of school that are much more secure. USB drives can only be used if they are encrypted by the IT department.

Another common method of transferring files was to send files in an attachment to yourself by email. This is more secure than USB drives but has the weakness that files need to be downloaded and saved onto the PC to be edited and therefore should also be avoided.

The recommended method of working on files outside of school or on personal devices in school is using the OneDrive, Google Drive or Remote Access functionality.

### Cloud Storage (OneDrive, Dropbox, Google Drive, etc)

There are many online storage services that allow users to upload or sync files to access anywhere or share with others, e.g. Dropbox, OneDrive (personal), Google Drive (personal) and many others. These services are designed for consumers to store data that is not covered by the Data Protection Act and therefore do not meet either the technical requirements for protecting data or comply with the requirement not to process data outside the EEA without proper safeguards. **Therefore, these services must not be used to store school data.**

The school provides two secure systems for storing data, these are Staff Drive (part of Office 365) and Google Drive (part of G-Suite). Each user at the Trust has their own login to these systems (email address and password) and each account has a private area for storing files. On mobile devices you can use the Staff Drive or Google Drive app and sign-in with your school email account. For personal PCs or laptops you should access Staff Drive and Google Drive through a web browser. The sync feature should not be used on personal devices as this stores files on the device which would therefore be at risk.

Google Drive, accessed using the Coombe email login is the only online areas that can be used to store school data.

### Remote Access

Certain staff members can use the remote-access system provided by the school. This establishes a secure connection to the school network and all access is through a computer on the school network. The great advantage of this is that no data is ever stored onto the device and therefore any device can be used regardless of the security on the device.

### Web Access

Many of the school systems can be accessed through a web browser such as email, Staff Drive and Google Drive. Like remote access, this method does not store data on the device so does not require the same level of security. Uses must be careful not to check the ‘remember me’, ‘keep me logged in’ or ‘remember my password’ box on sites, must sign-out after use and must be careful not to download documents onto the device.